ES-305

Intelligent Layer 2 Managed Switch

User's Guide

Version 1.0
6/2007
Edition 1

DEFAULT LOGIN	
IP Address	**http://192.168.0.1**

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ES-305 using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.
- Supporting Disk

  Refer to the included CD for support documents.
- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

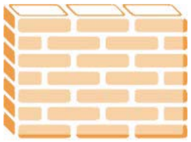
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The ES-305 may be referred to as the "ES-305", the "device", the "system", the "switch" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance** > **Log** > **Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ES-305 icon is not an exact representation of your device.

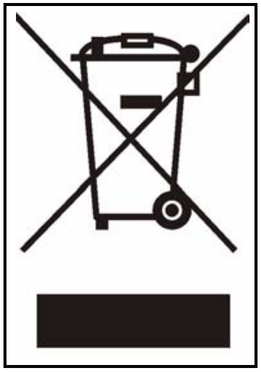
ES-305 	Computer 	Notebook computer
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

This product is recyclable. Dispose of it properly.



Contents Overview

Table of Contents

List of Figures

List of Tables

PART I
Introduction

1

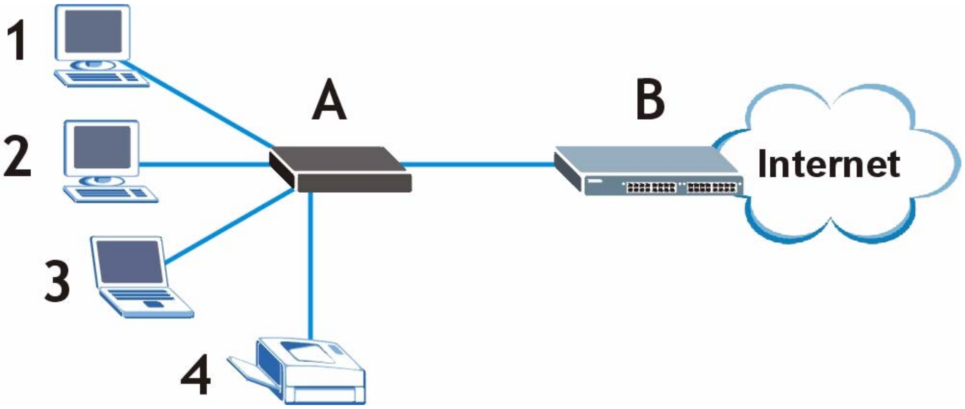
Introducing the ES-305

This chapter introduces the main applications and features of the ES-305. It also introduces the ways you can manage the ES-305.

1.1 Overview

The ES-305 is an intelligent five-port Ethernet switch. Use it to connect up to four devices to your network. The following figure shows the ES-305 (**A**) connecting several devices (**1** ~ **4**) and allowing them to communicate with one another and access the Internet through the Internet Service Provider's network switch (**B**).

Figure 1 Internet Access through the ES-305



1.2 Ways to Manage the ES-305

Use any of the following methods to manage the ES-305.

- Web Configurator. This is recommended for everyday management of the ES-305 using a (supported) web browser. See Chapter 2 on page 25.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup/restore.
- SNMP. The device can be monitored and/or managed by an SNMP manager.

1.3 Good Habits for Managing the ES-305

Do the following things regularly to make the ES-305 more secure and to manage the ES-305 more effectively.

- Change the username and password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ES-305 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ES-305. You could simply restore your last configuration.

1.4 LEDs

Figure 2 LEDs

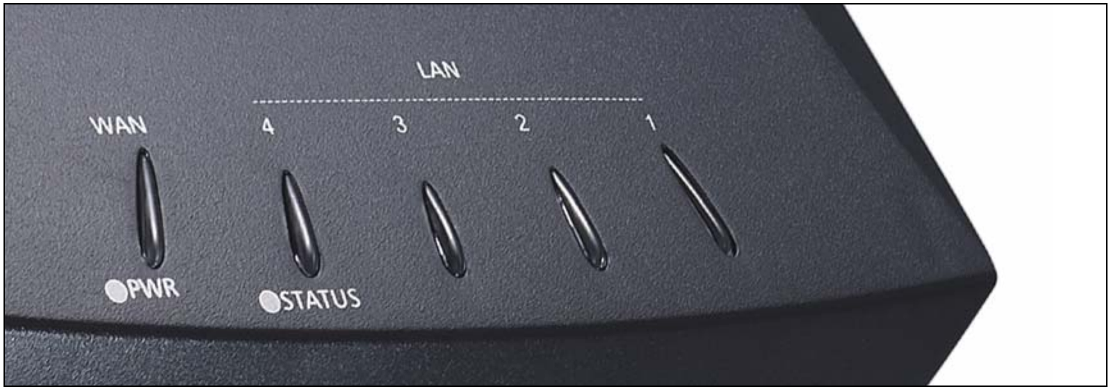


Table 1 LEDs

LED	STATUS		DESCRIPTION
WAN / PWR	Green	On	The power is on.
	Amber	On	The power is on and the ES-305 has a successful **WAN** port connection.
	Amber / Green	Blinking	The power is on, the ES-305 has a successful **WAN** port connection, and is sending or receiving data through the port.
	Off		The power is off.
LAN 4 / STATUS	Green	On	The ES-305 is starting up.
		Blinking	The ES-305 is operating normally, and has no Ethernet connection on the **LAN 4** port.
	Amber / Green	Blinking	The ES-305 is operating normally, and has a successful Ethernet connection on the **LAN 4** port. The LED blinks regularly when the ES-305 is operating normally, and also blinks when sending or receiving data through the **LAN 4** port.
	Off		The power is off, or the ES-305 has malfunctioned.

Table 1 LEDs (continued)

LED	STATUS		DESCRIPTION
LAN 1 ~ 3	Amber	On	The **LAN** port has a successful Ethernet connection.
		Blinking	The **LAN** port has a successful Ethernet connection, and is sending or receiving data through the port.
	Off		The **LAN** port is not connected, or the device to which it is connected is switched off.

2

Introducing the Web Configurator

This chapter describes how to access the ES-305's web configurator.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy setup and management of the ES-305 via an Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Refer to the appendices to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

1 Make sure your hardware is properly connected and prepare your computer or computer network to connect to the ES-305 (refer to the Quick Start Guide).

2 Launch your web browser.

3 Type "192.168.0.1" as the URL (default).

4 By default, the ES-305 has no username or password configured. Just click **OK** in the screen that appears.

It is strongly recommended that you set a username and password for the ES-305 as soon as possible. Otherwise, anyone can log in and make configuration changes. Use the **System** > **Administrator Settings** screen to set up login information (see Section 4.3 on page 47).

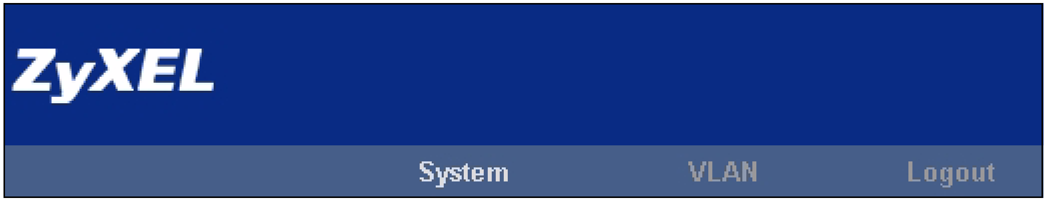
You should now see the **System Status** screen. See Section 4.1 on page 45 for details about this screen.

The management session automatically times out when the time period set in the **Idle Time Out** field in the **Administrator Settings** screen expires (default five minutes). Simply log back into the ES-305 if this happens.

2.3 Navigating the Web Configurator

The bar at the top of the screen contains several icons.

Figure 3 Top Bar Navigation Icons



- Click **System** to access screens allowing you to see system status information, make network configuration and administration changes, and perform maintenance tasks such as uploading firmware. See Chapter 5 on page 53 for information on the **System** screens.
- Click VLAN to access screens allowing you to set up Virtual LANs (VLANs) and assign network priority values on the ES-305. See Chapter 5 on page 53 for information on the **VLAN** screens.
- Click **Logout** at any time to exit the web configurator.

Click the Help button (Help) in any screen to see information about that screen.

3

Tutorial

This chapter describes how to configure your ES-305 in some example scenarios. It shows you how to do the following.

- Set up the ES-305 to use Virtual LANs (see Section 3.1 on page 27).
- Manage the ES-305 using Simple Network Management Protocol (see Section 3.2 on page 34).

3.1 How to Set Up Virtual LANs

This example shows you how to configure the ES-305 to use Virtual LANs (VLANs) in order to compartmentalize and prioritize data flows on your network. VLANs allow you to partition one physical network into separate virtual networks. Each VLAN behaves like its own network. Even though data from different VLANs may pass through the same physical cables, the different virtual networks do not exchange data.

You can use VLANs to allow certain computers to communicate only with other computers, to give certain computers higher priority on the network, or to have computers in different places act as if they were directly connected to one another.

VLAN-aware switches (like the ES-305) know which VLAN a data frame belongs to by reading its VLAN tag, which is a number from 1 to 4094 contained in the frame's header. Every frame belonging to a certain VLAN has the same identifying number. This number is called the VLAN ID, or VID.

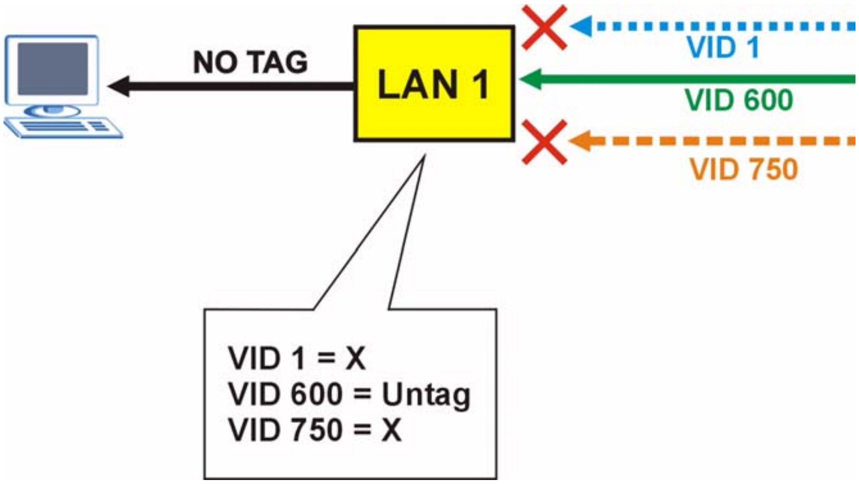
3.1.1 VLANs and the ES-305

The ES-305 lets you set up VLANs in two ways. In the **VLAN** > **VLAN Group Settings** screen, you can configure how the ES-305 deals with incoming frames by specifying which ports (**LAN 1** ~ **4** and **WAN**) can belong to which VLANs (a port can accept frames from more than one VLAN). In the **VLAN** > **Port VID Settings** screen, you can configure the VID that each port assigns to outgoing frames, as well as the priority level of these frames on the network.

3.1.1.1 VLAN Group Settings

The following figure shows how the **VLAN Group Settings** screen works. In this example, devices connected to the **LAN 1** port are able to be a member of VLAN **600**, but not VLAN **750** or **1**.

Figure 4 Tutorial: VLAN Group Settings Example

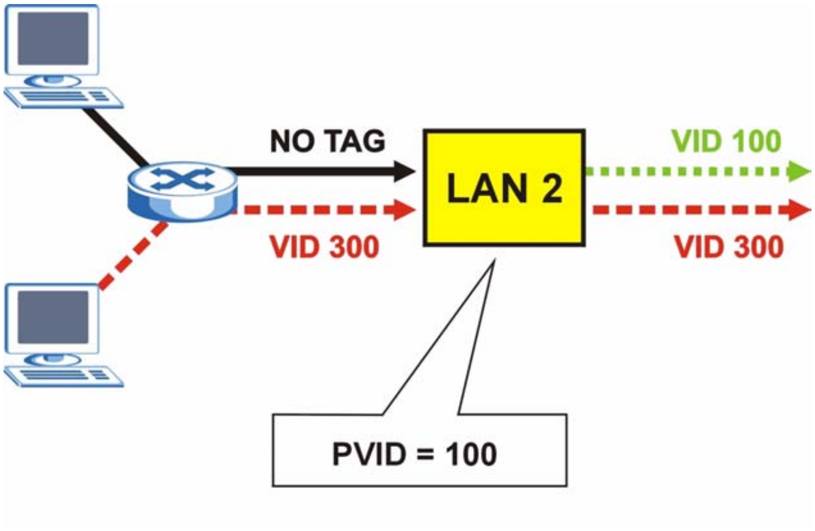


Incoming data from VLANs **1** and **750** is not transmitted. Incoming data from VLAN **600** is forwarded, but has its VLAN tag removed. This means that any device connected to **LAN 1** can see the data (if the VLAN tag had been kept, only devices also configured to be in that VLAN could see the data).

3.1.1.2 Port VID Settings

The following figure shows how the **Port VID Settings** screen works. In this example, some of the data frames on the **LAN 2** port arrive with VLAN information already in place, whereas other data frames do not have any. The ES-305 assigns a VLAN ID to the data frames without existing VLAN information.

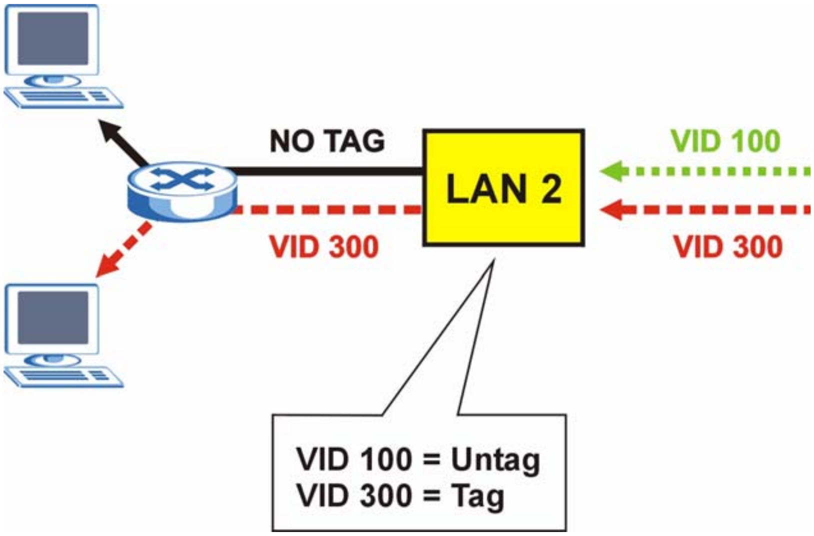
Figure 5 Tutorial: Port VID Settings Example



3.1.1.3 Combining Group VLAN and PVID Settings

When configuring VLAN settings on the ES-305, the settings in the **Group VLAN Settings** screen and the **Port VID Settings** screen must correspond. For instance, in the **Port VID Settings** example above (Section 3.1.1.2 on page 28) you would also configure a **Group VLAN Settings** screen rule allowing the **LAN 2** port to belong to VLANs **100** and **300**, and to keep VLAN **300**'s tag while removing the tag from VLAN 100. This rule is illustrated in the following figure.

Figure 6 Tutorial: Combining Group VLAN and PVID Settings



3.1.2 Example Scenario

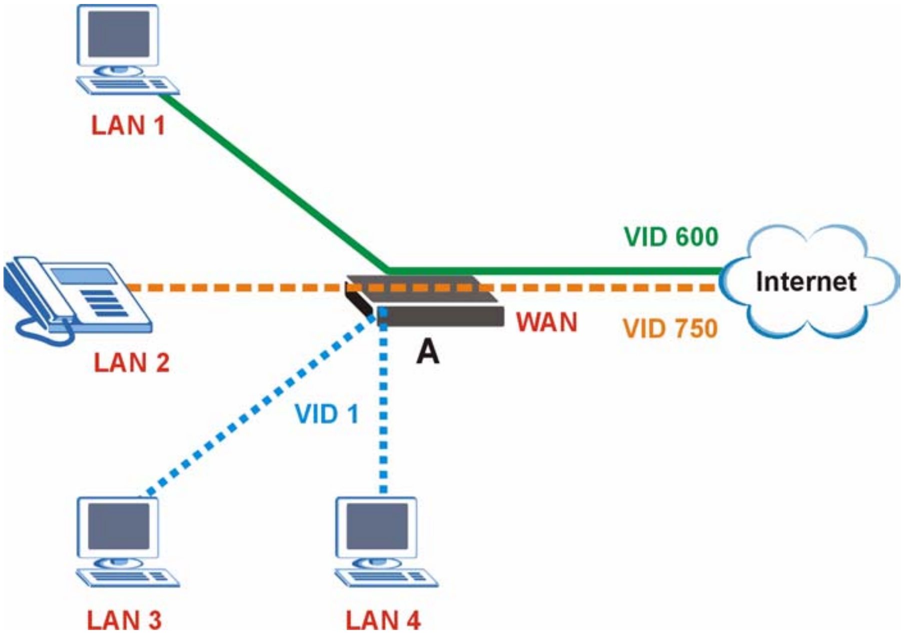
In this scenario, your Internet Service Provider (ISP) supplies you with Voice over IP (VoIP) telephone service, as well as standard Internet access. Each service is delivered along a separate VLAN. You want to set up your ES-305 to do the following things.

- Allow the ES-305 to be configured through ports 3 and 4 only.
- Provide standard Internet access through a single port, to which you will connect your computer.
- Provide VoIP service through a single port, to which you will connect an IP phone.
- Give the VoIP traffic the highest priority on the network.
- Allow other computers to communicate with one another through the ES-305, but to have access to neither Internet nor VoIP services.

Your ISP has told you that the Internet access VLAN has the VID **600**, and the VoIP VLAN has the VID **750**. The other VLAN exists entirely on your devices (not the ISP's) so you can use any number you like, as long as it does not conflict with either of the other VIDs. In this case, use VID **1** since it is already configured as the ES-305's default management VLAN.

The following figure shows your network, and the VLANs you want to set up. The computer connected to the **LAN 1** port on the ES-305 (**A**) can connect to the Internet, the IP phone connected to the **LAN 2 port** can connect to the VoIP service, and the computers connected to the **LAN 2** and **LAN 3** ports can communicate with one another.

Figure 7 Tutorial: Three VLANs

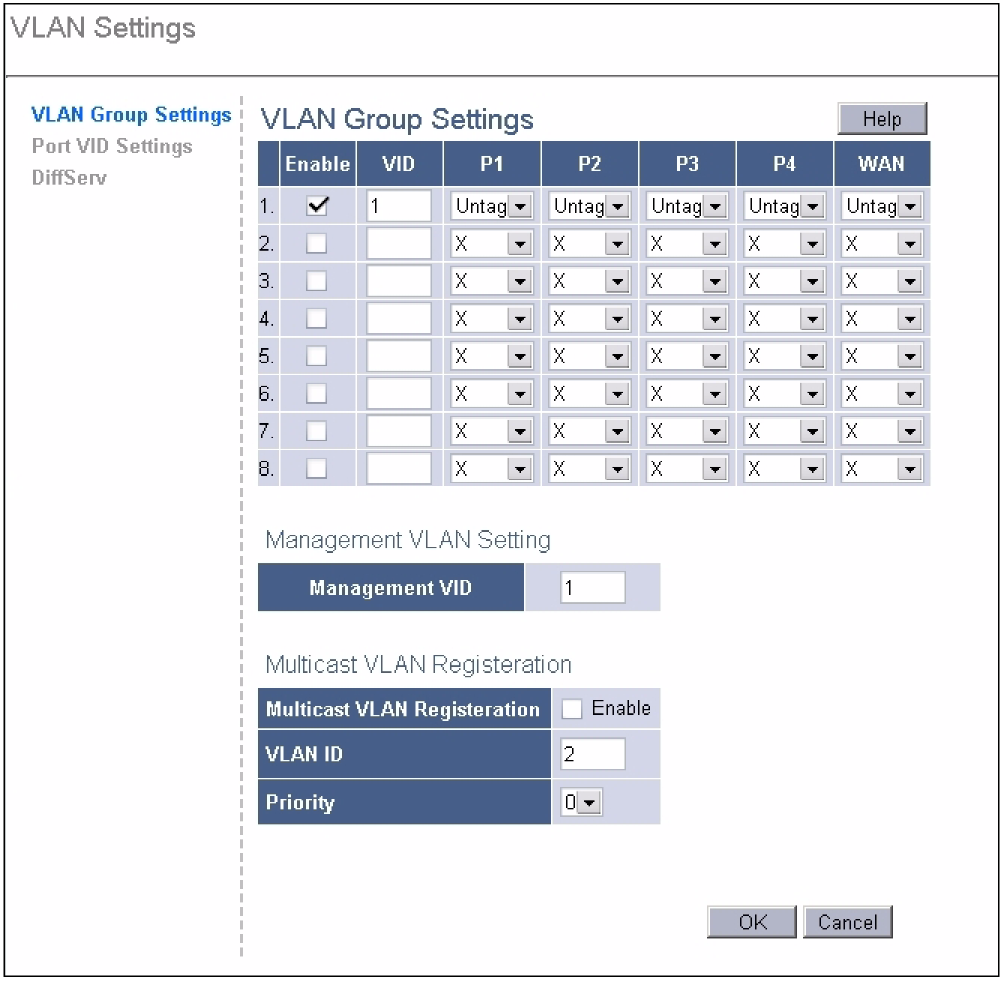


3.1.2.1 Configuring the Scenario

Take the following steps to configure this setup.

1. On a computer connected to the **LAN 3** or **4** port, log into the ES-305 (see your Quick Start Guide for how to do this). Click **VLAN** > **VLAN Group Settings**. Here you can define which ports accept incoming traffic for each of your VLANs.

Figure 8 Tutorial: VLAN Group Settings



VLAN Group Settings

	Enable	VID	P1	P2	P3	P4	WAN
1.	☑	1	Untag	Untag	Untag	Untag	Untag
2.	☐		X	X	X	X	X
3.	☐		X	X	X	X	X
4.	☐		X	X	X	X	X
5.	☐		X	X	X	X	X
6.	☐		X	X	X	X	X
7.	☐		X	X	X	X	X
8.	☐		X	X	X	X	X

Management VLAN Setting

Management VID	1

Multicast VLAN Registeration

Multicast VLAN Registeration	☐ Enable
VLAN ID	2
Priority	0

2 The first rule is the default preset rule that allows devices connected to any port to manage the ES-305 and freely exchange data. Do the following to modify the first rule to allow devices connected to the **LAN 3** and **4** ports to communicate with one another and manage the ES-305.

Make sure you set this rule up correctly! If you configure the ES-305 so that no ports are on the management VLAN, you cannot access it and will have to reset it to its factory default settings.

- Ensure that the **Enable** box is selected and **1** is entered in the **VID** field.
- Select **X** in the **LAN 1**, **2** and **WAN** columns. Leave the other columns at **Untag**.

3 Do the following to configure the second rule to allow devices connected to the **LAN 1** port to access the Internet through the **WAN** port.

- Select the **Enable** box, and enter **600** in the **VID** field.
- Select **Untag** in the rule's **P1** column (there are no VLAN-aware switches on that part of the network).

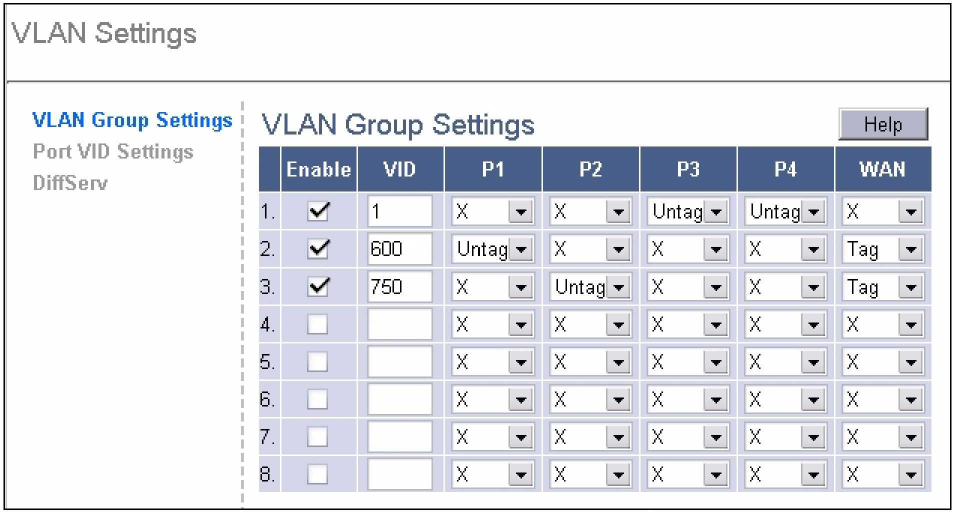
- Leave **LAN 2** ~ **4** at **X** (disable).
- Select **Tag** in the **WAN** column (there are VLAN-aware switches on that part of the network).

4 Configure the third rule to allow devices connected to the **LAN 2** port to access the VoIP service through the **WAN** port.

- Select the **Enable** box, and enter **750** in the **VID** field.
- Select **Untag** in the rule's **P2** column.
- Leave **LAN 1**, **3** and **4** at **X** (disable).
- Select **Tag** in the **WAN** column.

5 Click **Apply**.

Figure 9 Tutorial: VLAN Group Settings Complete



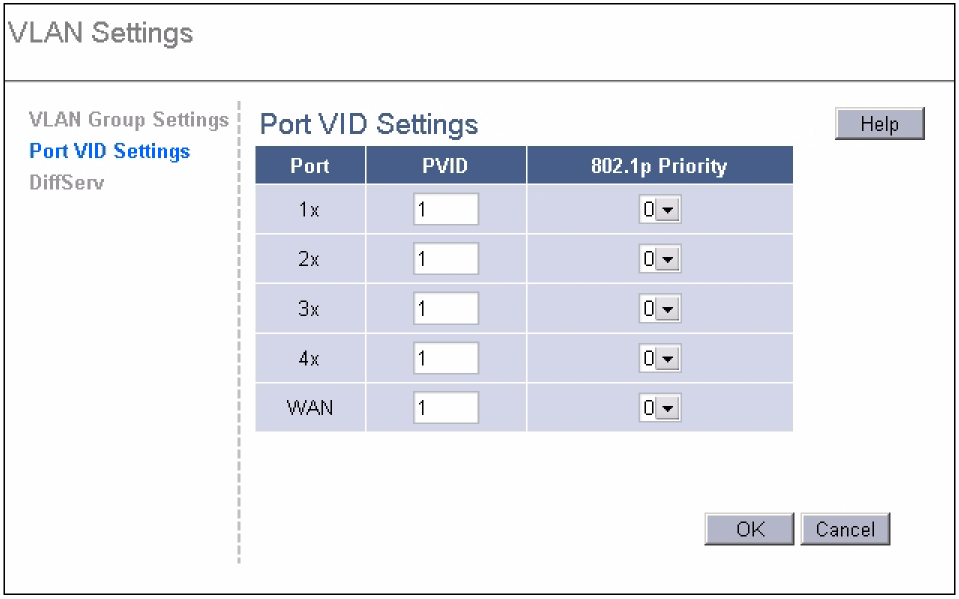
VLAN Group Settings

	Enable	VID	P1	P2	P3	P4	WAN
1.	☑	1	X	X	Untag	Untag	X
2.	☑	600	Untag	X	X	X	Tag
3.	☑	750	X	Untag	X	X	Tag
4.	□		X	X	X	X	X
5.	□		X	X	X	X	X
6.	□		X	X	X	X	X
7.	□		X	X	X	X	X
8.	□		X	X	X	X	X

6 Next, click **VLAN** > **Port VID Settings**. This screen allows you to specify the VLAN ID (VID) the ES-305 gives to data frames that arrive at each port without existing VLAN information.

In this screen, **1x** means the **LAN 1** port, and so on.

Figure 10 Tutorial: Port VID Settings



Port VID Settings

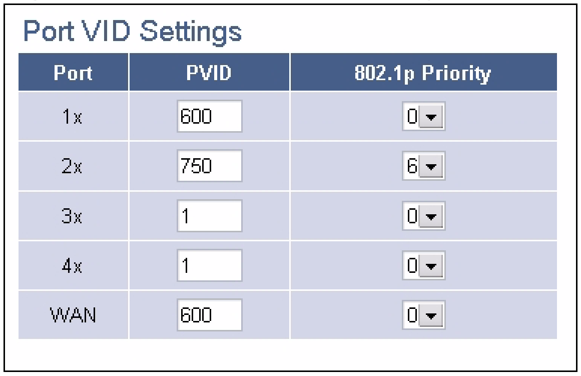
Port	PVID	802.1p Priority
1x	1	0
2x	1	0
3x	1	0
4x	1	0
WAN	1	0

7 Enter the following settings:

- In **1x**'s **PVID** field, enter **600**.
- In **2x**'s **PVID** field, enter **750**.
- In **3x**'s **PVID** field, enter **1**.
- In **4x**'s **PVID** field, enter **1**.
- In the **WAN** port's **PVID** field, enter **600**. In this scenario there should not be any traffic coming into the ES-305 on this port without a VLAN ID, but if there is it should be directed to LAN port 1. Furthermore, if you left the default PVID (1) the ES-305 could be managed through the WAN port.

8 Lastly, set the **802.1p Priority** field for **2x** to **6**. This gives the VoIP traffic on this port a very high priority.

Figure 11 Tutorial: Port VID Settings Screen Complete



Port VID Settings

Port	PVID	802.1p Priority
1x	600	0
2x	750	6
3x	1	0
4x	1	0
WAN	600	0

9 Click **OK**, then click **Continue** in the screen that appears. Congratulations! You are finished.

3.2 Using SNMP

SNMP Simple Network Management Protocol) is part of the TCP/IP networking suite. It allows a network administrator to remotely collect information about devices on the network, and make changes to their configuration. This tutorial is an example of using SNMP to monitor and manage a ZyXEL Device.

3.2.1 Requirements

In SNMP architecture, devices that issue requests for information are known as managers, and devices that provide information are known as agents. Agents can provide data to a manager either reactively (in response to a request) or autonomously (in the case of an alert). Each agent possesses a set of information types about which it can provide data, which is collectively known as a Management Information Base, or MIB.

To use SNMP on your network, you must obtain management software capable of issuing SNMP requests and displaying the returned responses. Many third-party SNMP managers exist, each of which is operated and displays information differently. However, the foundation upon which each is based is exactly the same.

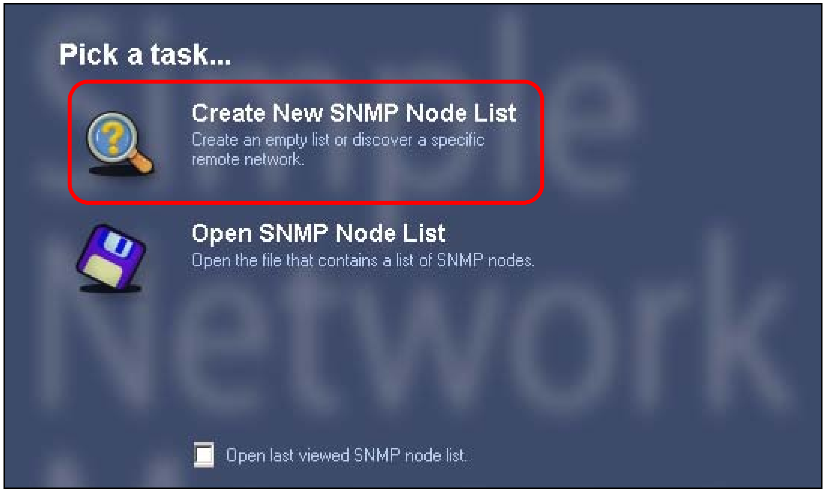
✍ This example uses SNMP Manager (v1.0.1.30) software manufactured by AdRem Software. It is presented in order to illustrate the capabilites of SNMP in conjunction with your ZyXEL device, but is NOT specifically a guide to using ZyXEL systems.

3.2.2 Discovering Your Device

When you use the SNMP manager for the first time, or add a new device to your network, you must either scan the network for SNMP-capable devices ("nodes") or specify each individual device's IP address. In this example, you will scan for nodes.

1 Open the SNMP manager. Click **Create New SNMP Node List**.

Figure 12 Tutorial: SNMP New Node List



Pick a task...

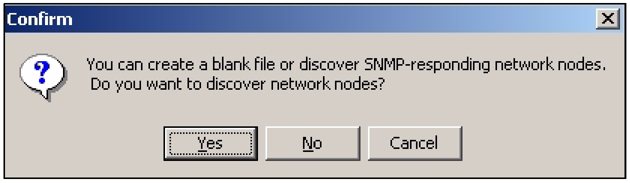
Create New SNMP Node List
Create an empty list or discover a specific remote network.

Open SNMP Node List
Open the file that contains a list of SNMP nodes.

□ Open last viewed SNMP node list.

2 A dialog box appears; click **Yes**.

Figure 13 Tutorial: SNMP Dialog Box

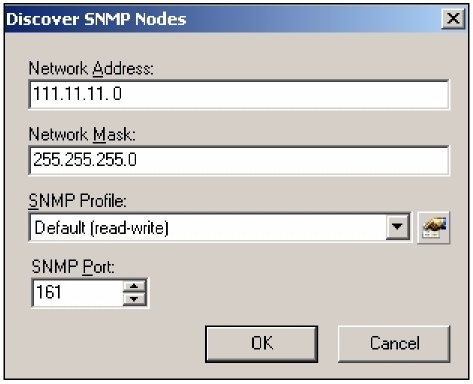


Confirm

You can create a blank file or discover SNMP-responding network nodes.
Do you want to discover network nodes?

3 The window that appears lets you specify an IP address range to scan, based on your computer's current IP address and subnet mask settings. You can also modify the SNMP port number (usually port 161). If you need to change the SNMP version or enter authentication details for your device, click the icon next to the **SNMP Profile** field. Unless you have a specific reason to change these settings, leave them at their defaults and click **OK**.

Figure 14 Tutorial: SNMP Node Discovery Window



Discover SNMP Nodes

Network Address: 111.11.11.0

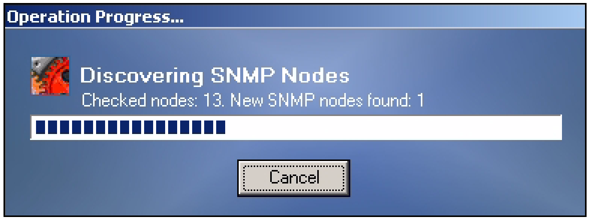
Network Mask: 255.255.255.0

SNMP Profile: Default (read-write)

SNMP Port: 161

A progress window displays as the SNMP manager searches for nodes.

Figure 15 Tutorial: SNMP Node Discovery Progress



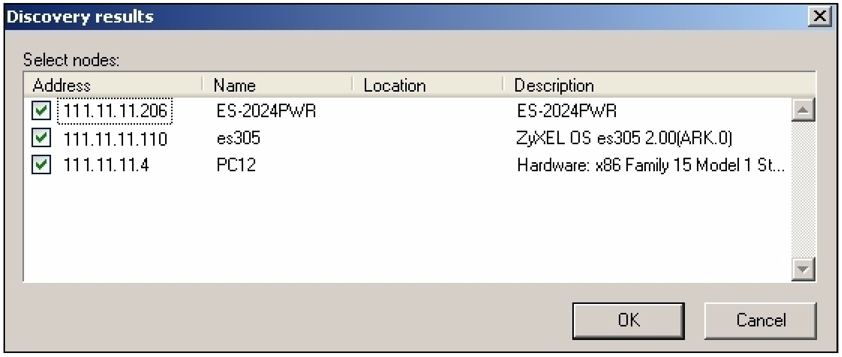
Operation Progress...

Discovering SNMP Nodes

Checked nodes: 13. New SNMP nodes found: 1

4 Once scanning is complete, a list of discovered nodes displays. Identify the device you want to manage either by its IP **Address**, **Name**, **Location**, or **Description**.

Figure 16 Tutorial: SNMP Discovered Nodes



Discovery results

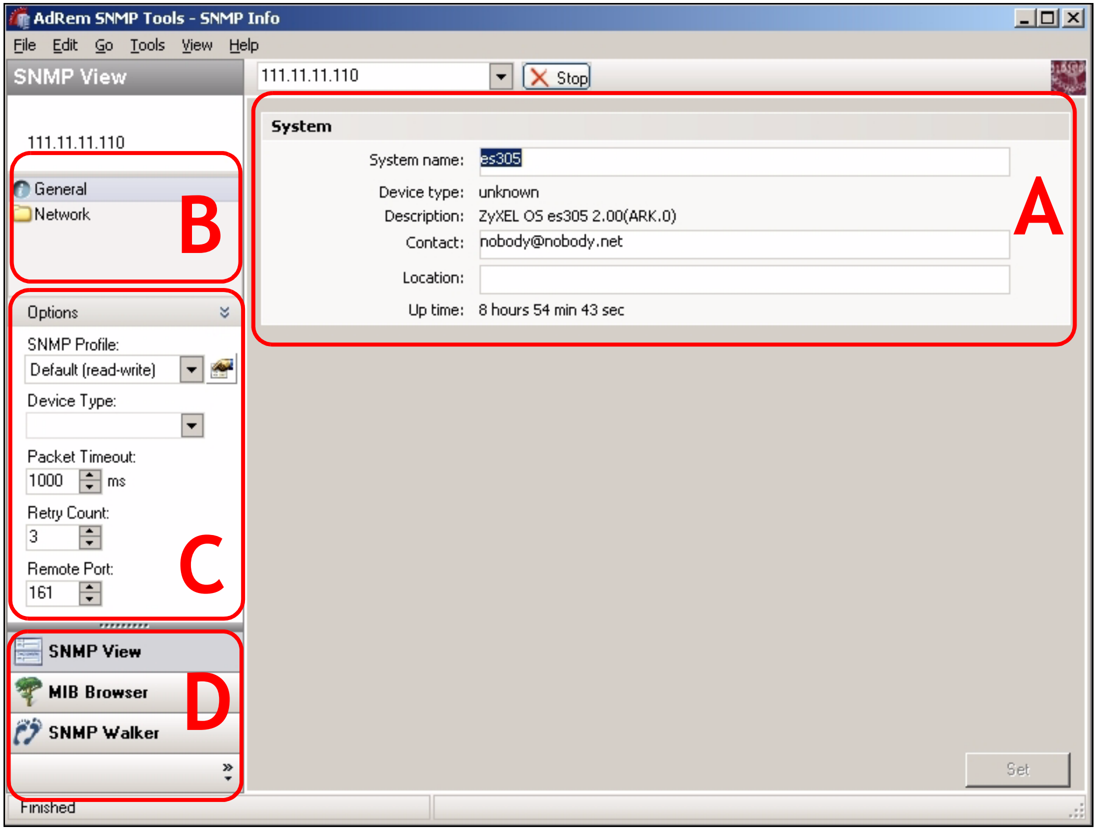
Select nodes:

Address	Name	Location	Description
☑ 111.11.11.206	ES-2024PWR		ES-2024PWR
☑ 111.11.11.110	es305		ZyXEL OS es305 2.00(ARK.0)
☑ 111.11.11.4	PC12		Hardware: x86 Family 15 Model 1 St...

3.2.3 Viewing SNMP Data

Once you have discovered all the SNMP-capable devices on your network, double-click the icon of the device you want to manage. The **SNMP Info** window displays, showing basic information about the device.

Figure 17 Tutorial: SNMP Info



System name: es305

Device type: unknown

Description: ZyXEL OS es305 2.00(ARK.0)

Contact: nobody@nobody.net

Location:

Up time: 8 hours 54 min 43 sec

SNMP Profile: Default (read-write)

Device Type:

Packet Timeout: 1000 ms

Retry Count: 3

Remote Port: 161

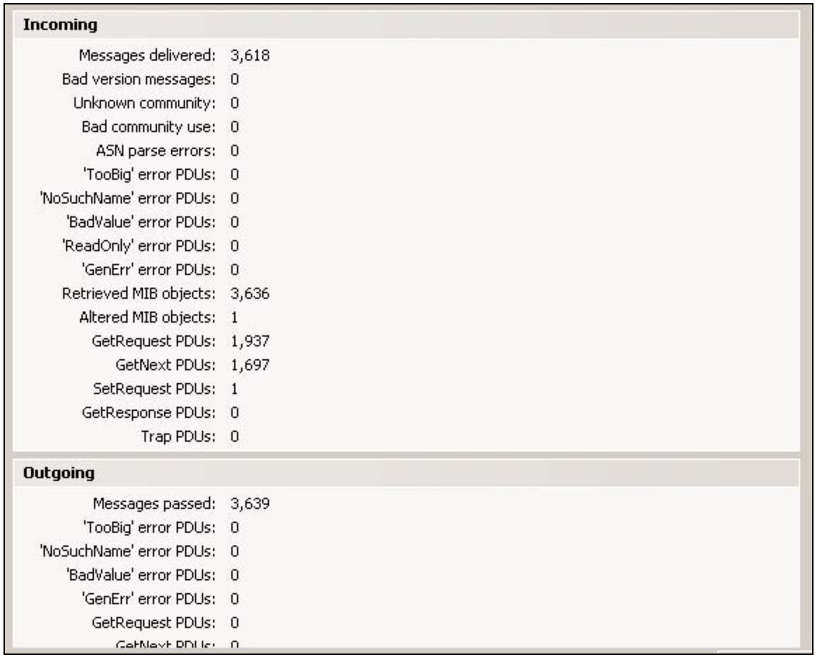
The panel on the right (**A**) shows the gathered data, and the panel on the left allows you to navigate (**B**) from one page of information to another, make changes to the way you access the SNMP agent (**C**), and use different management tools (**D**).

The following sections illustrate some of the functions provided by the ZyXEL Device's SNMP agent.

3.2.3.1 Viewing SNMP Statistics

To see statistics about the data provided by the ZyXEL Device's SNMP agent, double-click **Network** in the manager's navigation panel. The following screen displays, showing information on incoming and outgoing SNMP data.

Figure 18 Tutorial: SNMP Statistics



Incoming

Messages delivered:	3,618
Bad version messages:	0
Unknown community:	0
Bad community use:	0
ASN parse errors:	0
'TooBig' error PDUs:	0
'NoSuchName' error PDUs:	0
'BadValue' error PDUs:	0
'ReadOnly' error PDUs:	0
'GenErr' error PDUs:	0
Retrieved MIB objects:	3,636
Altered MIB objects:	1
GetRequest PDUs:	1,937
GetNext PDUs:	1,697
SetRequest PDUs:	1
GetResponse PDUs:	0
Trap PDUs:	0

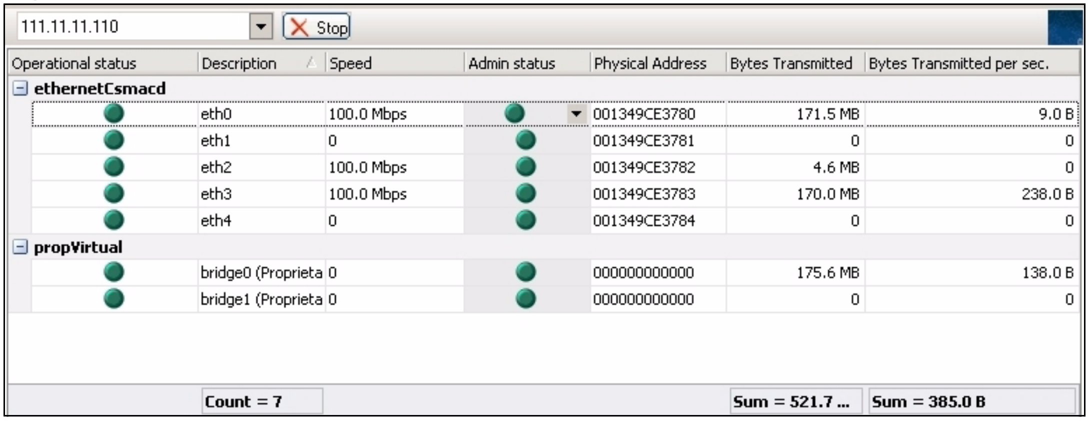
Outgoing

Messages passed:	3,639
'TooBig' error PDUs:	0
'NoSuchName' error PDUs:	0
'BadValue' error PDUs:	0
'GenErr' error PDUs:	0
GetRequest PDUs:	0
GetNext PDUs:	0

3.2.3.2 Viewing Interface Information

This section illustrates an example of viewing information about the ZyXEL Device's Ethernet ports, such as operational status, speed, and transmission / reception data. Click **Network** > **Interfaces** > **Basic Info**. The following screen displays, showing information on physical and virtual ports.

Figure 19 Tutorial: SNMP Interfaces



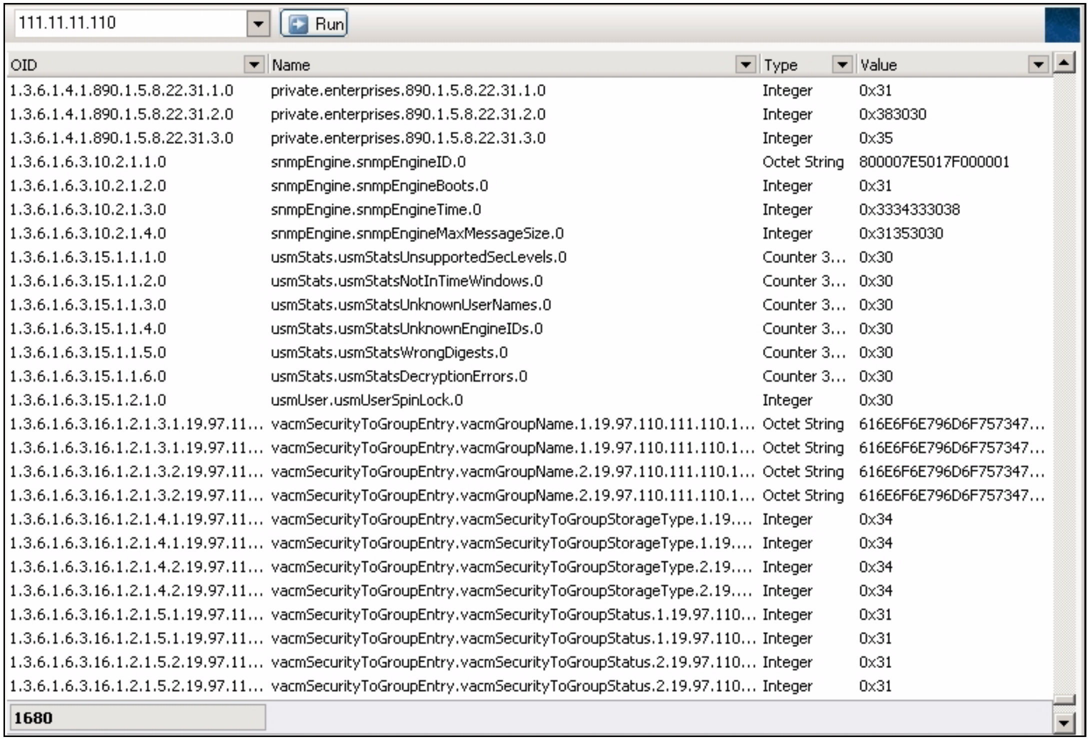
Operational status	Description	Speed	Admin status	Physical Address	Bytes Transmitted	Bytes Transmitted per sec.
⊟ **ethernetCsmacd**						
●	eth0	100.0 Mbps	●	001349CE3780	171.5 MB	9.0 B
●	eth1	0	●	001349CE3781	0	0
●	eth2	100.0 Mbps	●	001349CE3782	4.6 MB	0
●	eth3	100.0 Mbps	●	001349CE3783	170.0 MB	238.0 B
●	eth4	0	●	001349CE3784	0	0
⊟ **propVirtual**						
●	bridge0 (Proprieta	0	●	000000000000	175.6 MB	138.0 B
●	bridge1 (Proprieta	0	●	000000000000	0	0
	Count = 7				**Sum = 521.7 ...**	**Sum = 385.0 B**

3.2.3.3 SNMP Walk

The SNMP Walk feature allows you to discover all the types of SNMP data that can be supplied by your ZyXEL Device's SNMP agent. Each individual type of information has a unique OID (Object IDentifier) and name, which uniquely identify it in the MIB.

Click the **SNMP Walker** button and select the IP address of your ZyXEL Device from the list. Click **Run**. A screen similar to the following displays.

Figure 20 Tutorial: SNMP Walk



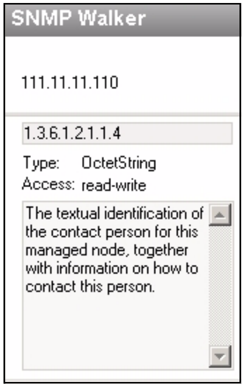
OID	Name	Type	Value
1.3.6.1.4.1.890.1.5.8.22.31.1.0	private.enterprises.890.1.5.8.22.31.1.0	Integer	0x31
1.3.6.1.4.1.890.1.5.8.22.31.2.0	private.enterprises.890.1.5.8.22.31.2.0	Integer	0x383030
1.3.6.1.4.1.890.1.5.8.22.31.3.0	private.enterprises.890.1.5.8.22.31.3.0	Integer	0x35
1.3.6.1.6.3.10.2.1.1.0	snmpEngine.snmpEngineID.0	Octet String	800007E5017F000001
1.3.6.1.6.3.10.2.1.2.0	snmpEngine.snmpEngineBoots.0	Integer	0x31
1.3.6.1.6.3.10.2.1.3.0	snmpEngine.snmpEngineTime.0	Integer	0x3334333038
1.3.6.1.6.3.10.2.1.4.0	snmpEngine.snmpEngineMaxMessageSize.0	Integer	0x31353030
1.3.6.1.6.3.15.1.1.1.0	usmStats.usmStatsUnsupportedSecLevels.0	Counter 3...	0x30
1.3.6.1.6.3.15.1.1.2.0	usmStats.usmStatsNotInTimeWindows.0	Counter 3...	0x30
1.3.6.1.6.3.15.1.1.3.0	usmStats.usmStatsUnknownUserNames.0	Counter 3...	0x30
1.3.6.1.6.3.15.1.1.4.0	usmStats.usmStatsUnknownEngineIDs.0	Counter 3...	0x30
1.3.6.1.6.3.15.1.1.5.0	usmStats.usmStatsWrongDigests.0	Counter 3...	0x30
1.3.6.1.6.3.15.1.1.6.0	usmStats.usmStatsDecryptionErrors.0	Counter 3...	0x30
1.3.6.1.6.3.15.1.2.1.0	usmUser.usmUserSpinLock.0	Integer	0x30
1.3.6.1.6.3.16.1.2.1.3.1.19.97.11...	vacmSecurityToGroupEntry.vacmGroupName.1.19.97.110.111.110.1...	Octet String	616E6F6E796D6F757347...
1.3.6.1.6.3.16.1.2.1.3.1.19.97.11...	vacmSecurityToGroupEntry.vacmGroupName.1.19.97.110.111.110.1...	Octet String	616E6F6E796D6F757347...
1.3.6.1.6.3.16.1.2.1.3.2.19.97.11...	vacmSecurityToGroupEntry.vacmGroupName.2.19.97.110.111.110.1...	Octet String	616E6F6E796D6F757347...
1.3.6.1.6.3.16.1.2.1.3.2.19.97.11...	vacmSecurityToGroupEntry.vacmGroupName.2.19.97.110.111.110.1...	Octet String	616E6F6E796D6F757347...
1.3.6.1.6.3.16.1.2.1.4.1.19.97.11...	vacmSecurityToGroupEntry.vacmSecurityToGroupStorageType.1.19....	Integer	0x34
1.3.6.1.6.3.16.1.2.1.4.1.19.97.11...	vacmSecurityToGroupEntry.vacmSecurityToGroupStorageType.1.19....	Integer	0x34
1.3.6.1.6.3.16.1.2.1.4.2.19.97.11...	vacmSecurityToGroupEntry.vacmSecurityToGroupStorageType.2.19....	Integer	0x34
1.3.6.1.6.3.16.1.2.1.4.2.19.97.11...	vacmSecurityToGroupEntry.vacmSecurityToGroupStorageType.2.19....	Integer	0x34
1.3.6.1.6.3.16.1.2.1.5.1.19.97.11...	vacmSecurityToGroupEntry.vacmSecurityToGroupStatus.1.19.97.110...	Integer	0x31
1.3.6.1.6.3.16.1.2.1.5.1.19.97.11...	vacmSecurityToGroupEntry.vacmSecurityToGroupStatus.1.19.97.110...	Integer	0x31
1.3.6.1.6.3.16.1.2.1.5.2.19.97.11...	vacmSecurityToGroupEntry.vacmSecurityToGroupStatus.2.19.97.110...	Integer	0x31
1.3.6.1.6.3.16.1.2.1.5.2.19.97.11...	vacmSecurityToGroupEntry.vacmSecurityToGroupStatus.2.19.97.110...	Integer	0x31

1680

3.2.3.4 OID Descriptions

When you click on an entry in the **SNMP Walk** list, a short description displays in the panel on the left of the screen. For example, if you click an entry with the OID “1.3.6.1.2.1.1.4.0” and the name “system.sysContact.0”, the description reads “The textual identification of the contact person for this managed node, together with information on how to contact this person.”

Figure 21 Tutorial: SNMP OID Description



111.11.11.110

1.3.6.1.2.1.1.4

Type: OctetString

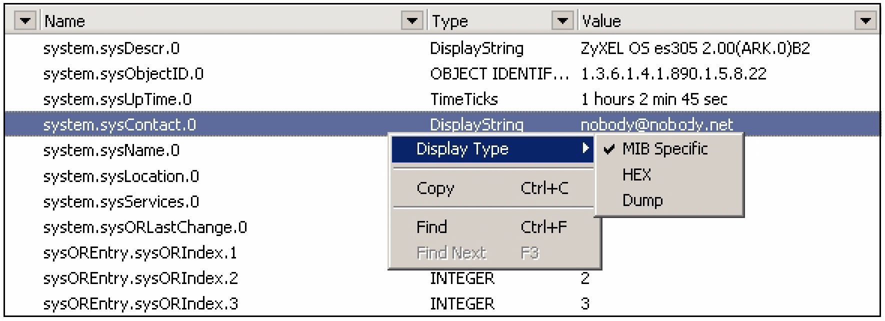
Access: read-write

The textual identification of the contact person for this managed node, together with information on how to contact this person.

3.2.3.5 MIB-Specific Display

To read the specific information provided by the device’s MIB, right-click in the right-hand panel and select **Display** > **MIB Specific** from the menu that appears. The fields in the **Value** column change, displaying the values provided by the device’s MIB in an easily-readable format.

Figure 22 Tutorial: SNMP MIB-Specific Display Type



Name	Type	Value
system.sysDescr.0	DisplayString	ZyXEL OS es305 2.00(ARK.0)B2
system.sysObjectID.0	OBJECT IDENTIF...	1.3.6.1.4.1.890.1.5.8.22
system.sysUpTime.0	TimeTicks	1 hours 2 min 45 sec
system.sysContact.0	DisplayString	nobody@nobody.net
system.sysName.0		
system.sysLocation.0		
system.sysServices.0		
system.sysORLastChange.0		
sysOREntry.sysORIndex.1		
sysOREntry.sysORIndex.2	INTEGER	2
sysOREntry.sysORIndex.3	INTEGER	3

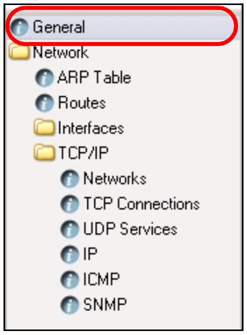
3.2.4 Making Changes

Some fields can be modified in the SNMP manager, whereas others are read-only. When you modify fields, the SNMP manager issues commands to the ZyXEL Device’s SNMP agent, instructing it to make configuration changes. Fields that can be modified can be visually identified as such in the SNMP manager interface.

For example, take the following steps to change the basic information about your ZyXEL Device (the device name, location, contact person, and so on).

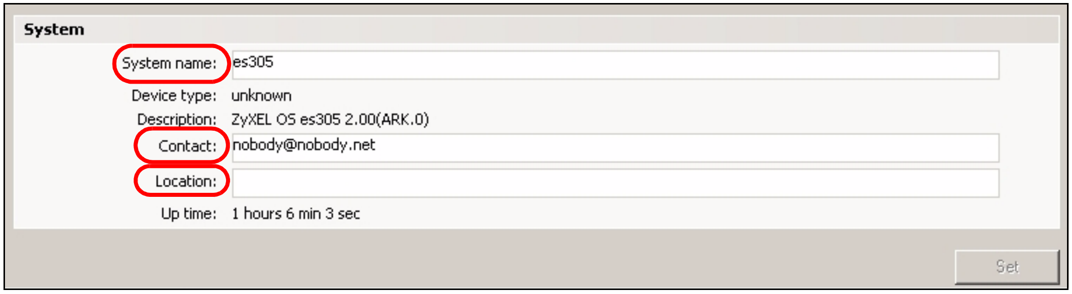
1 If you are not already in the **SNMP View** mode, click the **SNMP View** button. Go to the MIB navigation panel and click **General**.

Figure 23 Tutorial: SNMP View > General



The following screen displays. The **System name**, **Contact** and **Location** fields can be modified.

Figure 24 Tutorial: SNMP General System Information

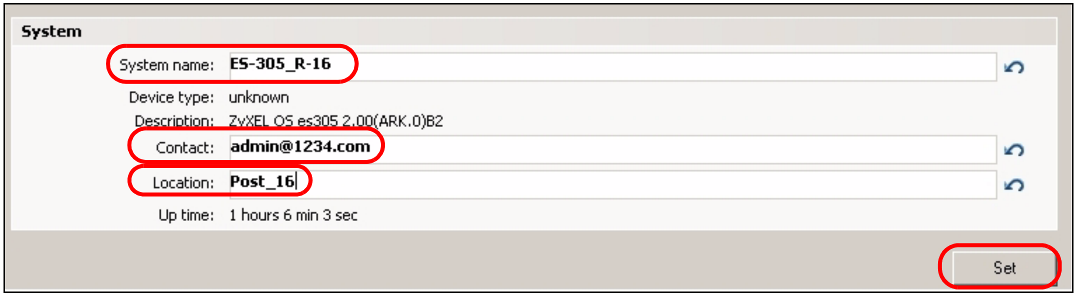


System

System name: es305
Device type: unknown
Description: ZyXEL OS es305 2.00(ARK.0)
Contact: nobody@nobody.net
Location:
Up time: 1 hours 6 min 3 sec

2 Enter the new information in the fields and click **Set**.

Figure 25 Tutorial: SNMP New Information



System

System name: ES-305_R-16

Device type: unknown

Description: ZyXEL OS es305 2.00(ARK.0)B2

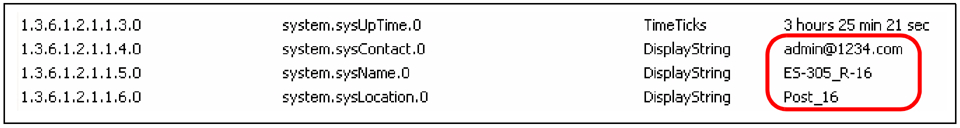
Contact: admin@1234.com

Location: Post_16

Up time: 1 hours 6 min 3 sec

3 The next time you check the information (using the SNMP Walk feature, for example) you can see that the changes have been made.

Figure 26 Tutorial: SNMP Changes Made



```
1.3.6.1.2.1.1.3.0    system.sysUpTime.0      TimeTicks       3 hours 25 min 21 sec
1.3.6.1.2.1.1.4.0    system.sysContact.0     DisplayString   admin@1234.com
1.3.6.1.2.1.1.5.0    system.sysName.0        DisplayString   ES-305_R-16
1.3.6.1.2.1.1.6.0    system.sysLocation.0    DisplayString   Post_16
```

PART II
Web Configurator and Troubleshooting

4

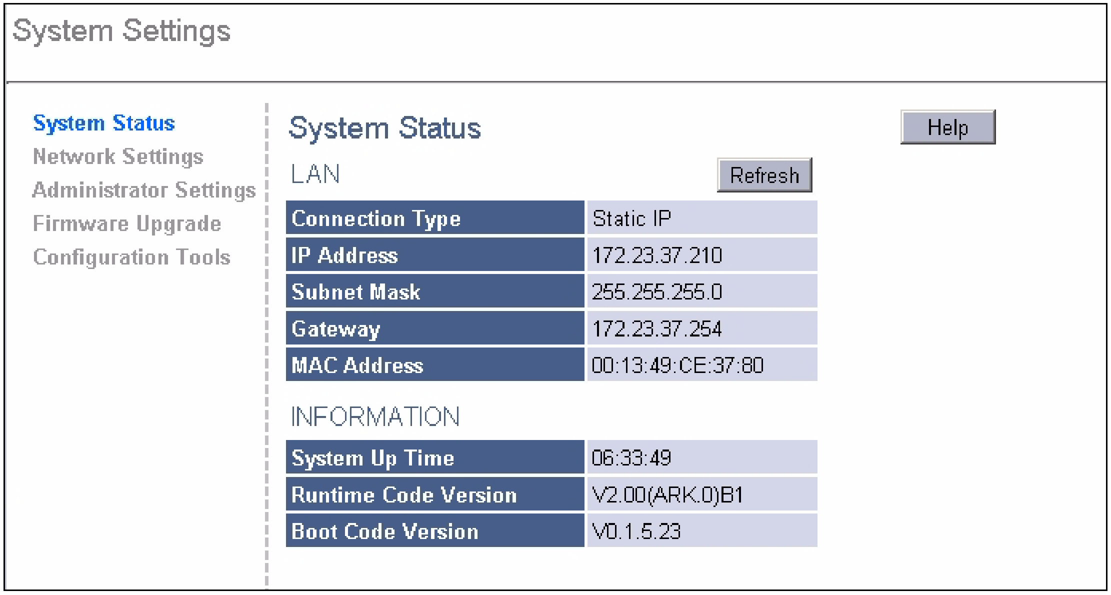
System Screens

This chapter discusses the ES-305's **System** screens.

4.1 The System Status Screen

This screen displays details of the ES-305 User's Guide's LAN settings and management information. Click **System** > **System Status**. The following screen displays.

Figure 27 System Status



Connection Type	Static IP
IP Address	172.23.37.210
Subnet Mask	255.255.255.0
Gateway	172.23.37.254
MAC Address	00:13:49:CE:37:80
System Up Time	06:33:49
Runtime Code Version	V2.00(ARK.0)B1
Boot Code Version	V0.1.5.23

The following table describes the labels in this screen.

Table 2 System Status

LABEL	DESCRIPTION
Refresh	Click this to update the information in this screen.
LAN	These fields contain read-only details of the ES-305's LAN IP settings. You can configure these settings in the **System** > **Network Settings** screen.
Connection Type	This field displays whether the ES-305 is set to get an IP address automatically (**DHCP**) or uses an IP address you configure manually (**Static IP**)
IP Address	This field displays the IP address currently configured on the ES-305.
Subnet Mask	This field displays the subnet mask currently configured on the ES-305.

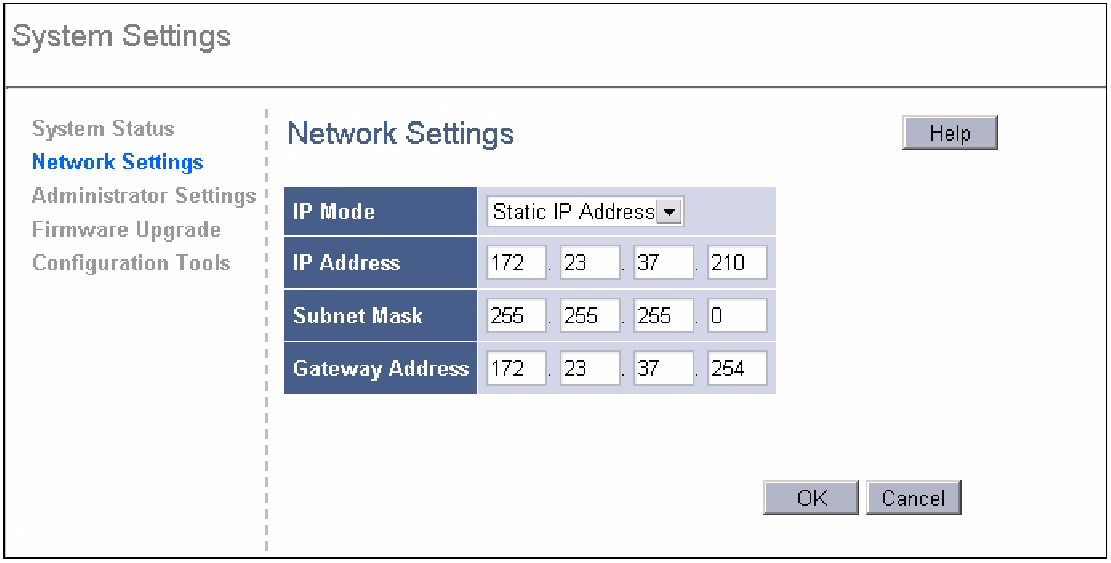
Table 2 System Status

LABEL	DESCRIPTION
Gateway	This field displays the IP address of the gateway currently configured on the ES-305. The gateway is the network node that allows devices connected to the ES-305 to access another network (the Internet, for example).
MAC Address	This field displays the Media Access Control (MAC) address of the ES-305. Every networking device has a unique MAC address, which identifies it.
Information	These fields contain read-only details of the firmware currently running on the ES-305, and the amount of time since it was switched on.
System Up Time	This shows the elapsed time since the ES-305 was switched on.
Runtime Code Version	This is the version number of the runtime code (also known as the firmware code) currently installed on the ES-305. You can upload new firmware in the **System** > **Firmware Upgrade** screen.
Boot Code Version	This is the version number of the boot code currently installed on the ES-305.

4.2 The Network Settings Screen

Use this screen to configure the ES-305's IP settings. Click **System** > **Network Settings**. The following screen displays.

Figure 28 Network Settings



IP Mode	Static IP Address
IP Address	172 . 23 . 37 . 210
Subnet Mask	255 . 255 . 255 . 0
Gateway Address	172 . 23 . 37 . 254

The following table describes the labels in this screen.

Table 3 Network Settings

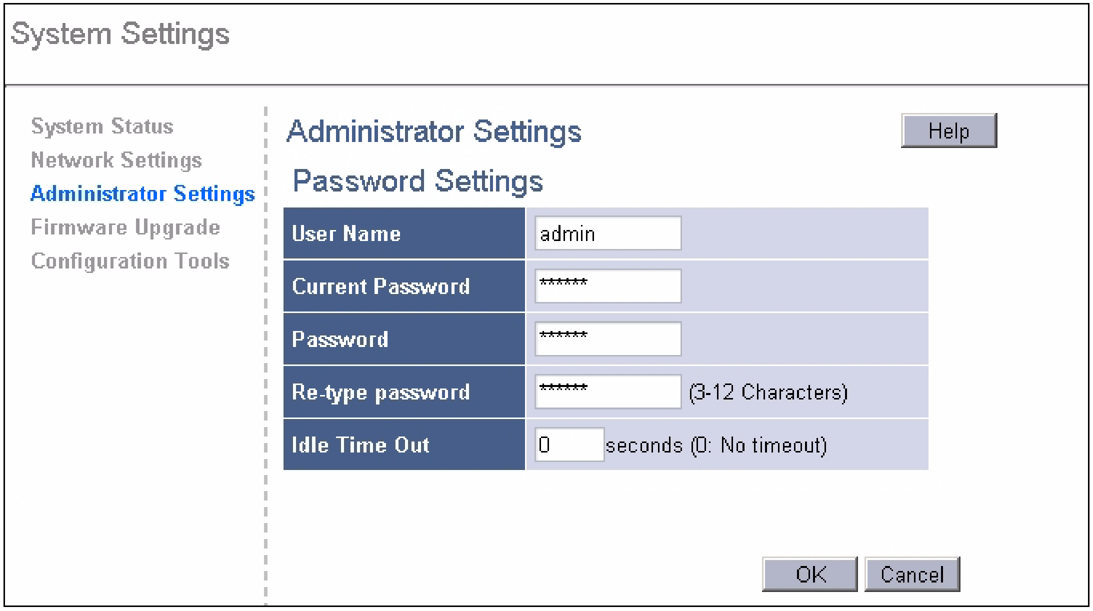
LABEL	DESCRIPTION
IP Mode	Select **DHCP Mode** if you have a DHCP server that can assign the ES-305 an IP address, subnet mask, default gateway IP address and a domain name server address automatically. Select **Static IP address** if you don't have a DHCP server, or if you wish to assign static IP address information to the ES-305. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your ES-305 in dotted decimal notation (for example, 192.168.0.1).
Subnet Mask	Enter the IP subnet mask of your ES-305 in dotted decimal notation (for example, 255.255.255.0).
Gateway Address	Enter the IP address of the default outgoing gateway in dotted decimal notation (for example, 192.168.0.254).
OK	Click this to save your changes.
Cancel	Click this to return the fields in this screen to their last-saved settings.

4.3 The Administrator Settings Screen

Use this screen to change the username and password information used to access the ES-305's web configurator. You can also set the idle timeout in this screen.

Click **System** > **Administrator Settings**. The following screen displays.

Figure 29 Administrator Settings



User Name	admin
Current Password	******
Password	******
Re-type password	****** (3-12 Characters)
Idle Time Out	0 seconds (0: No timeout)

The following table describes the labels in this screen.The following table describes the labels in this screen.

Table 4 Administrator Settings

LABEL	DESCRIPTION
User Name	Enter the administrator user name for accessing the ES-305's web configurator.
Current Password	Enter the password already configured on the ES-305. If no password is configured, leave this field blank.
Password	Enter the new password you want to use.
Re-type password	Re-enter the new password exactly as you typed it before.
Idle Time Out	Type how many seconds a management session (via the web configurator) can be left idle before the session times out (closes). If the session times out, you have to log in to the web configurator again. Very long timeouts may have security risks.
OK	Click this to save your changes.
Cancel	Click this to return the fields in this screen to their last-saved settings.

4.4 The Firmware Upgrade Screen

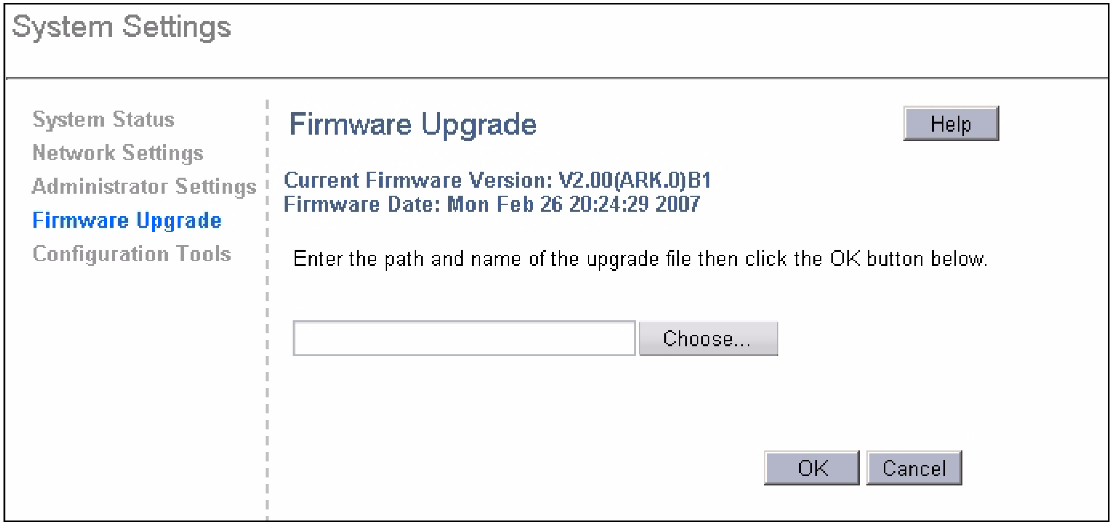
Use this screen to upload new firmware to the ES-305. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

Use firmware for your device's specific model only. Refer to the label on the bottom of your ES-305.

Click **System** > **Firmware Upgrade**. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system reboots.

Do NOT turn off the ES-305 while firmware upload is in progress!

Figure 30 Firmware Upgrade



Current Firmware Version: V2.00(ARK.0)B1
Firmware Date: Mon Feb 26 20:24:29 2007

Enter the path and name of the upgrade file then click the OK button below.

The following table describes the labels in this screen.

Table 5 Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This field displays the version number of the firmware currently installed on the ES-305. This also displays in the **System** > **System Status** screen as the **Runtime Code Version**.
Firmware Date	This field displays the date of the firmware currently installed on the ES-305.
Choose...	Click this to locate the firmware file you wish to upload to the ES-305. Remember that you must decompress compressed (.zip) files before you can upload them.
OK	Click this to upload the new firmware. A warning window appears to check whether you really want to upgrade.
Cancel	Click this to return the fields in this screen to their last-saved values.

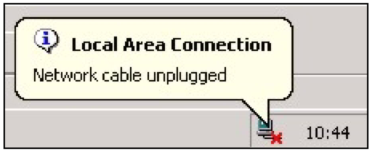
After you see the **Firmware Upload in Progress** screen, wait two minutes before logging into the ES-305 again.

Figure 31 Firmware Upload In Progress

Uploading..
-

The ES-305 automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

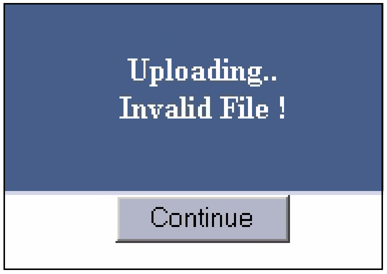
Figure 32 Network Temporarily Disconnected


Local Area Connection
Network cable unplugged

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware Upgrade** screen.

Figure 33 Error Message



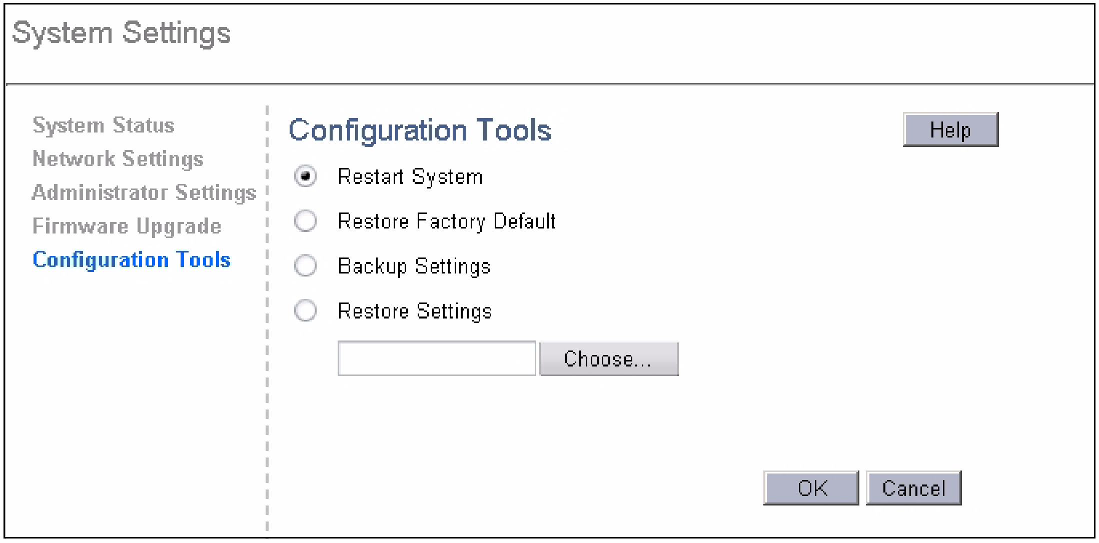
Uploading..
Invalid File !

4.5 The Configuration Tools Screen

Use this screen to perform various administrative tasks such as backing up the ES-305's configuration and resetting the it to its factory default settings.

Click **System** > **Configuration Tools**. The following screen displays.

Figure 34 Configuration Tools



System Settings

Configuration Tools

● Restart System

○ Restore Factory Default

○ Backup Settings

○ Restore Settings

The following table describes the labels in this screen.

Table 6 Configuration Tools

LABEL	DESCRIPTION
Restart System	Select this to turn the ES-305 off, then on. The settings on the ES-305 remain unchanged.
Restore Factory Defaults	Select this to return the ES-305 to its factory default settings. Its IP address will be 192.168.0.1 and the administrator username and password will be set.

Table 6 Configuration Tools

LABEL	DESCRIPTION
Backup Settings	Select this to back up (save) the ES-305’s current configuration to a file on your computer. The backup configuration file will be useful in case you need to return to your previous settings. Note: Once your ES-305 is configured and functioning properly, it is strongly recommended that you back up your configuration file before making configuration changes.
Restore Settings	Select this to upload a new or previously-saved configuration file from your computer to your ES-305. After you see an “OK!” screen, click **Continue** and log in again when prompted. Note: Do NOT turn off the ES-305 while configuration file upload is in progress!
Choose	Click this to select the configuration file you want to upload when you select **Restore Settings**.
OK	Click this to perform the selected task.
Cancel	Click this to return the fields in this screen to their previously-saved values.

5

VLAN Screens

This chapter describes the ES-305's VLAN (Virtual Local Area Network) screens.

5.1 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the switch on which they were created. The VLANs can be created statically by hand or dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible number of VLAN configurations is 4,094.

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits

5.1.1 Forwarding Tagged and Untagged Frames

Each port on the switch is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the switch first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

5.1.2 Management VLAN ID

If you want to access the ES-305 (for configuration, for example) you must connect to it through a port that is a member of the management VLAN. If a port is not a member of the management VLAN, devices connected through it cannot access the ES-305. The management VLAN ID is the identifying number (1 ~ 4094) of the management VLAN. All ports are in the management VLAN (the default management VLAN ID is 1) by default.

> If you set all the ports on the ES-305 to not be in the management VLAN, you cannot access the ES-305. You will need to reset it to its factory default settings if you want to make configuration changes.

5.1.3 Multicast VLAN Registration

Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand, or MoD) using multicast traffic across an Ethernet network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management. MVR is also known as Multicast VLAN Group (MVG).

5.1.4 DiffServ

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

5.1.5 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP (6 bits)	Unused (2 bits)

DSCP is backwards-compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

5.2 The VLAN Group Settings Screen

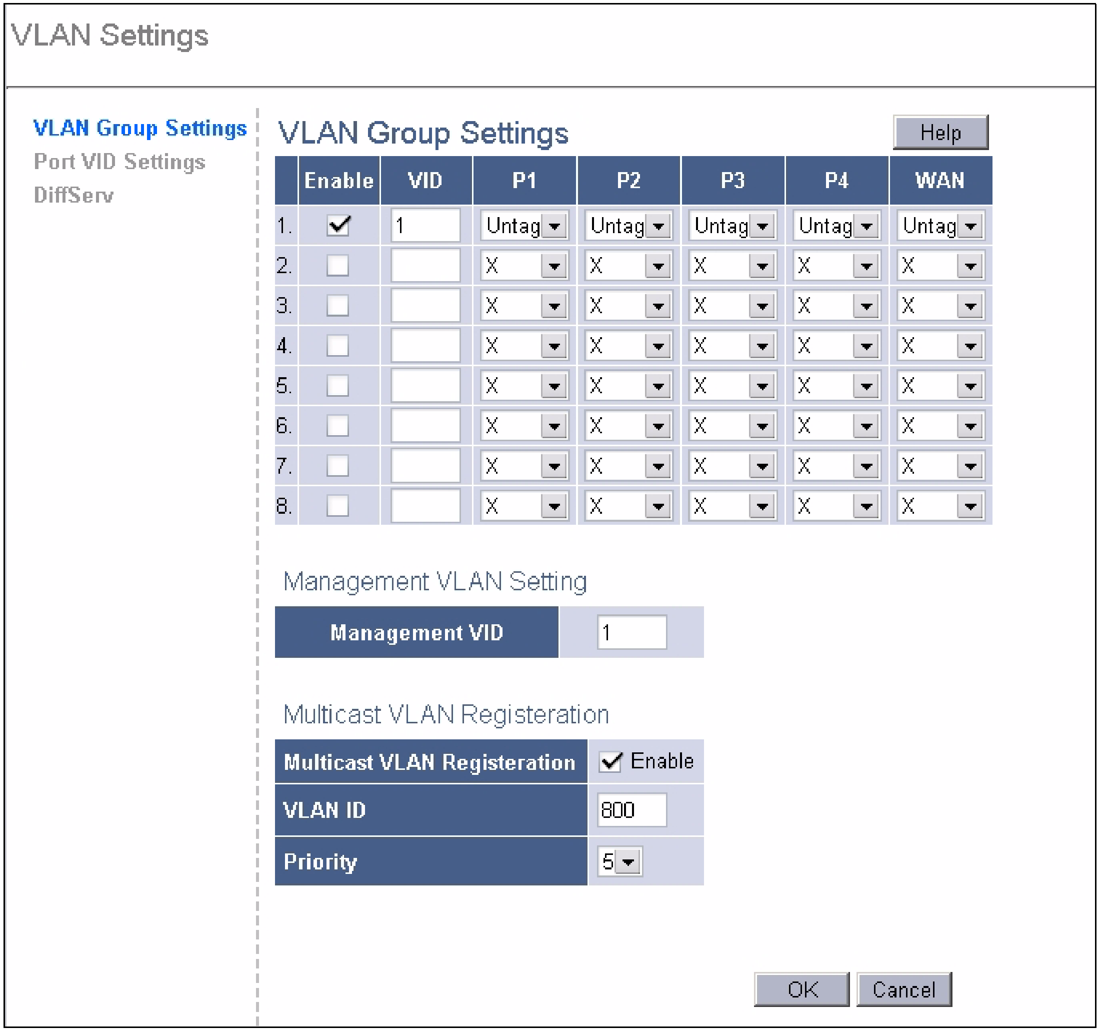
Use this screen to set up IEEE 802.1Q VLAN tagging on the ES-305. You can configure up to eight VLAN rules. Each rule allows you to specify how each port deals with incoming packets. Use VLAN group setting rules to specify whether a port is:

- A member of a VLAN. Packets are forwarded with VLAN tags.
- A member of a VLAN. Packets are forwarded without VLAN tags.
- Not a member of a VLAN.

✍ If you block incoming traffic tagged with the management VLAN ID (the default is **1**) on a port, devices on that port cannot access the ES-305. If you block all ports from accessing the ES-305, you must reset the ES-305 if you want to access its web configurator.

Click **VLAN** > **VLAN Group Settings**. The following screen displays.

Figure 35 VLAN Group Settings



VLAN Group Settings

	Enable	VID	P1	P2	P3	P4	WAN
1.	☑	1	Untag	Untag	Untag	Untag	Untag
2.	□		X	X	X	X	X
3.	□		X	X	X	X	X
4.	□		X	X	X	X	X
5.	□		X	X	X	X	X
6.	□		X	X	X	X	X
7.	□		X	X	X	X	X
8.	□		X	X	X	X	X

Management VLAN Setting

Management VID	1

Multicast VLAN Registeration

Multicast VLAN Registeration	☑ Enable
VLAN ID	800
Priority	5

The following table describes the labels in this screen.

Table 7 VLAN Group Settings

LABEL	DESCRIPTION
Enable	Select this to have the ES-305 use the rule. Leave it unselected if you do not want to use the rule.
VID	Enter the VLAN ID for this rule (1 ~ 4094).
P1 ~ P4, WAN	Select one of the following to configure the state of each of the ES-305's ports: • **X**: This indicates that the port is not part of the VLAN. • **Tag**: This indicates that the port is a member of the VLAN. When the packet leaves the member port, the VLAN tag is added. • **Untag**: This indicates that this port is a member of the VLAN. When the packet leaves the member port, the VLAN tag is removed.

Table 7 VLAN Group Settings

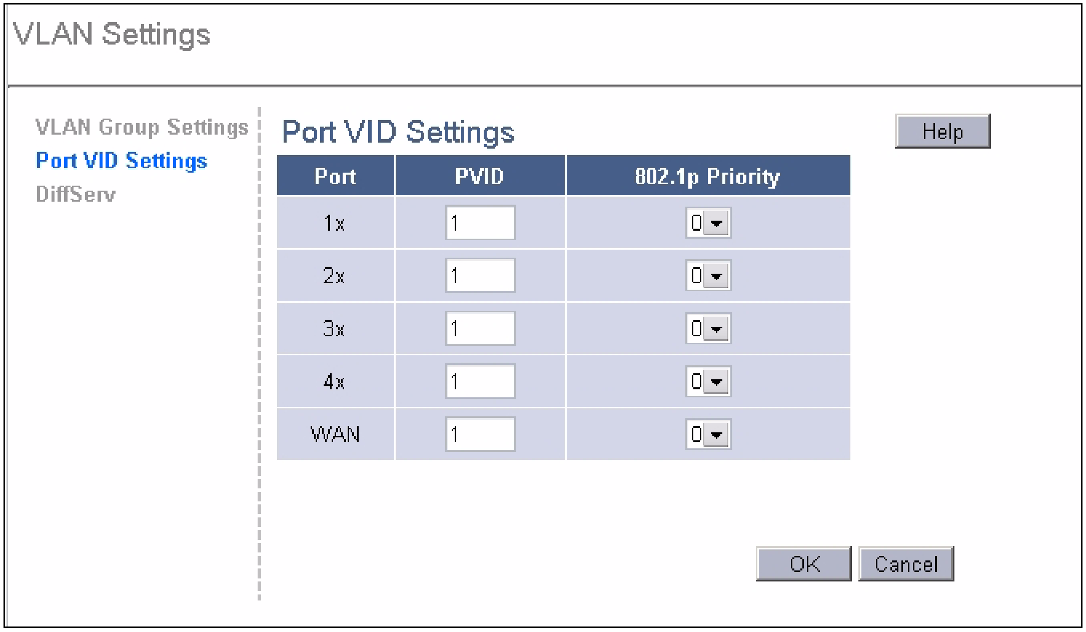
LABEL	DESCRIPTION
Management VID	The management VLAN is used for accessing the ES-305. Only devices connected to ports that are members of the management VLAN can access the ES-305. Enter the VLAN identification number associated with the ES-305. The default is **1**. All ports are members of the management VLAN by default. Note: If no port is a member of this VLAN, you cannot access the ES-305.
Multicast VLAN registration	Multicast VLAN Registration (MVR) allows multiple users to subscribe to a multicast VLAN stream (television service, for example) while remaining in separate VLANs. Select **Enable** to subscribe to the multicast VLAN stream you configure in the **VLAN ID** field.
VLAN ID	Enter the multicast VLAN ID (1 ~ 4094).
Priority	Enter the 802.1p priority level for multicast VLAN traffic.
OK	Click this to save your changes.
Cancel	Click this to return this screen to its last-saved settings.

5.3 The Port VID Screen

Use this screen to configure the VLAN ID (VID) of each port on the ES-305. The ES-305 assigns a PVID (Port VLAN ID) and IEEE 802.1p priority level to outgoing untagged traffic from each port. If the traffic already possesses an IEEE 802.1Q VLAN tag, it is not changed.

Click **VLAN** > **Port VID** Settings. The following screen displays.

Figure 36 Port VID Settings



Port VID Settings

Port	PVID	802.1p Priority
1x	1	0
2x	1	0
3x	1	0
4x	1	0
WAN	1	0

The following table describes the labels in this screen.

Table 8 Port VID Settings

LABEL	DESCRIPTION
Port	This column displays the port name. (LAN **1x** ~ **4x** and **WAN**)
PVID	This column displays the Port VLAN ID. Enter the VLAN ID (1 ~ 4094) for untagged traffic on each port. Note: If you enter a VLAN ID different from the management VLAN ID (see Section 5.2 on page 55) devices connected to the this port cannot access the ES-305 for management, unless they already possess the correct VLAN tag.
802.1p Priority	Select a priority level (0-7) for the ES-305 to assign to packets on each port. A higher number indicates a higher priority.
OK	Click this to save your changes.
Cancel	Click this to return the screen to its last-saved settings.

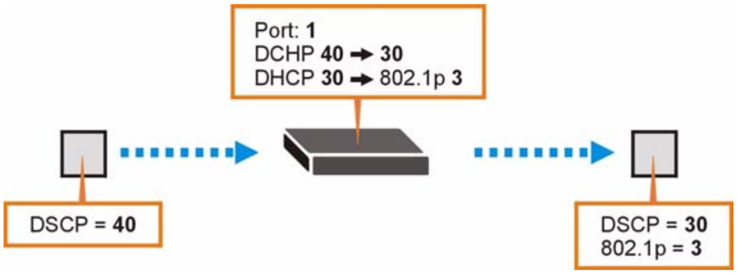
5.4 The DiffServ Screen

Use this screen to enable and configure DiffServ Code Point (DSCP) and DSCP / IEEE 802.1p priority mapping on each of the ES-305’s ports.

DSCP Code Point mapping allows you to change the priority of incoming packets (if you want to connect two DiffServ networks, for example). IEEE 802.1p priority mapping allows you to assign an 802.1p priority value to a packet based on its DSCP value.

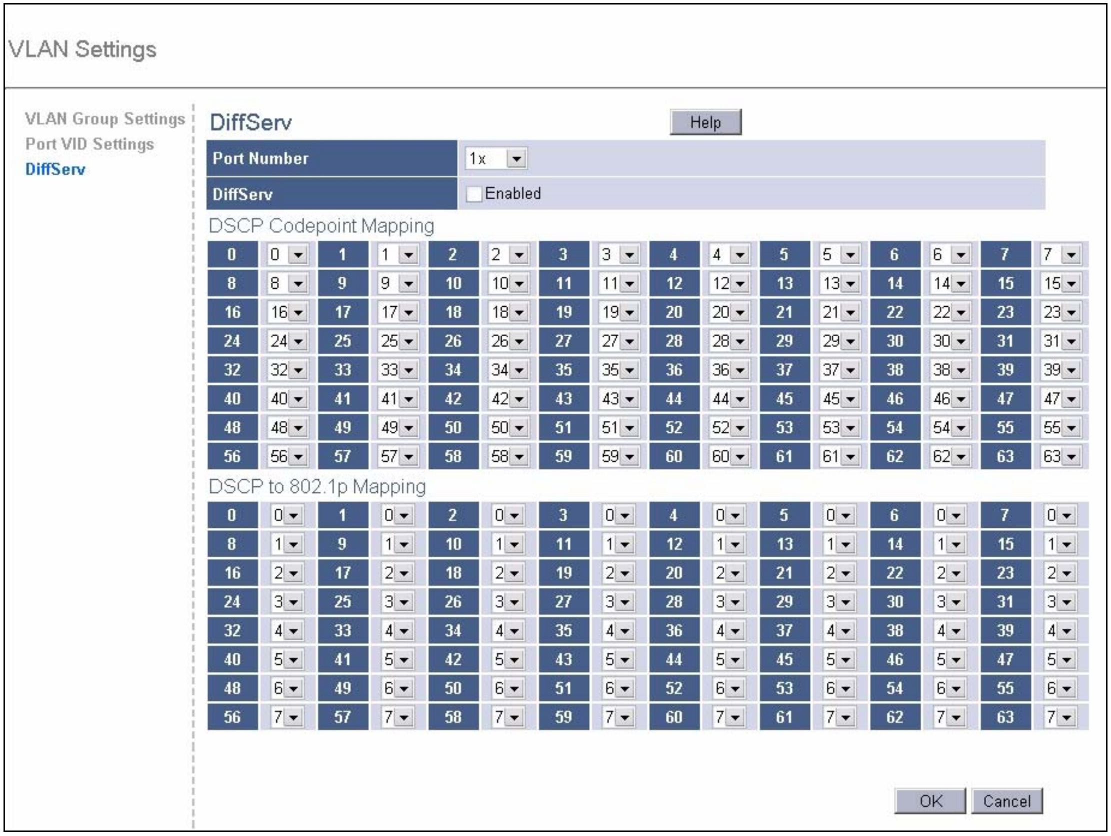
The following example shows an incoming packet on port 1 with a DSCP value of 40. The DSCP code point mapping rule for port 1 alters DSCP value from 40 to 30, and the IEEE 802.1p priority mapping rule assigns a 802.1p value of 3, based on the new DSCP value.

Figure 37 DiffServ Example



Click **VLAN** > **DiffServ**. The following screen displays.

Figure 38 Diffserv



DiffServ

Port Number: 1x

DiffServ: □ Enabled

DSCP Codepoint Mapping

0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7
8	8	9	9	10	10	11	11	12	12	13	13	14	14	15	15
16	16	17	17	18	18	19	19	20	20	21	21	22	22	23	23
24	24	25	25	26	26	27	27	28	28	29	29	30	30	31	31
32	32	33	33	34	34	35	35	36	36	37	37	38	38	39	39
40	40	41	41	42	42	43	43	44	44	45	45	46	46	47	47
48	48	49	49	50	50	51	51	52	52	53	53	54	54	55	55
56	56	57	57	58	58	59	59	60	60	61	61	62	62	63	63

DSCP to 802.1p Mapping

0	0	1	0	2	0	3	0	4	0	5	0	6	0	7	0
8	1	9	1	10	1	11	1	12	1	13	1	14	1	15	1
16	2	17	2	18	2	19	2	20	2	21	2	22	2	23	2
24	3	25	3	26	3	27	3	28	3	29	3	30	3	31	3
32	4	33	4	34	4	35	4	36	4	37	4	38	4	39	4
40	5	41	5	42	5	43	5	44	5	45	5	46	5	47	5
48	6	49	6	50	6	51	6	52	6	53	6	54	6	55	6
56	7	57	7	58	7	59	7	60	7	61	7	62	7	63	7

The following table describes the labels in this screen.

Table 9 DiffServ

LABEL	DESCRIPTION
Port Number	Select the port (LAN **1x** ~**4x** or **WAN**) you want to configure.
DiffServ	Select **Enable** to have the port assign DiffServ Code Point (DSCP) values. Leave this unselected if you do not want to use this feature.
DSCP Codepoint Mapping	The ES-305 can change the DSCP (DiffServ Code Point) value of incoming packets prior to sending them to their destinations. For each incoming DSCP value you want to change on this port, select the new value from the list.
DSCP to 802.1p Mapping	The ES-305 can assign an IEEE 802.1p value based on a packet's DSCP value. If the DSCP value is changed in the **DSCP Codepoint Mapping** fields of this screen, the new value is used for 802.1p mapping.
OK	Click this to save your changes.
Cancel	Click this to return this screen to its last-saved values.

6

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ES-305 Access and Login
- Internet Access
- Resetting the ES-305 to Its Factory Defaults

6.1 Power, Hardware Connections, and LEDs

? The ES-305 does not turn on. None of the LEDs turn on.

1 Make sure you are using the power adaptor or cord included with the ES-305.
2 Make sure the power adaptor or cord is connected to the ES-305 and plugged in to an appropriate power source. Make sure the power source is turned on.
3 Disconnect and re-connect the power adaptor or cord to the ES-305.
4 If the problem continues, contact the vendor.

? One of the LEDs does not behave as expected.

1 Make sure you understand the normal behavior of the LED. See Section 1.4 on page 22.
2 Check the hardware connections. See the Quick Start Guide.
3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4 Disconnect and re-connect the power adaptor to the ES-305.
5 If the problem continues, contact the vendor.

6.2 ES-305 Access and Login

I forgot the IP address for the ES-305.

1. The default IP address is **192.168.0.1**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 6.4 on page 64.

I forgot the password.

1. The ES-305 has no password or username by default. Try just clicking **OK** when you are asked for your login details.
2. If this does not work, you have to reset the device to its factory defaults. See Section 6.4 on page 64.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.0.1.
   - If you changed the IP address (Section 4.2 on page 46), use the new IP address.
   - If you changed the IP address and have forgotten it, you have to reset the device to its factory defaults. See Section 6.4 on page 64.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 22.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 75.
4. Make sure your computer is in the same subnet as the ES-305. (If you know that there are routers between your computer and the ES-305, skip this step.)
   - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ES-305. See Section 6.1 on page 61.
5. Reset the device to its factory defaults, and try to access the ES-305 with the default IP address. See Section 6.4 on page 64.
6. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try connecting your computer to another of the ES-305's ports. The ES-305 may be set to forbid management access on one or more ports. If management is forbidden on all ports, you must reset the ES-305. See Section 6.4 on page 64.

I can see the **Login** screen, but I cannot log in to the ES-305.

1. Make sure you have entered the user name and password correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on. The ES-305 has no user name or password by default, so try just clicking **OK** when you are asked for your login information.
2. You cannot log in to the web configurator while someone is using the web configurator or Telnet to access the ES-305. Log out of the ES-305 in the other session, or ask the person who is logged in to log out.
3. Disconnect and re-connect the power adaptor or cord to the ES-305.
4. If this does not work, you have to reset the device to its factory defaults. See Section 6.4 on page 64.

I cannot Telnet to the ES-305.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

6.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 22.
2. Ensure that any information you entered in the **Network Settings** screen (such as an IP address) is correct. If you changed the default VLAN settings, ensure that they are properly configured, or return them to the default configuration (see Section 6.4 on page 64 for how to reset the ES-305).
3. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
4. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ES-305), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.4 on page 22.
2 Disconnect and re-connect the power adaptor to the ES-305.
3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.4 on page 22. If the ES-305 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2 Disconnect and re-connect the power adaptor to the ES-305.
3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the 802.1p and DiffServ settings in the **VLAN** screens. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

6.4 Resetting the ES-305 to Its Factory Defaults

If you reset the ES-305, you lose all of the changes you have made. The ES-305 re-loads its default settings. You have to make all of your changes again.

You will lose all of your changes when you push the **RESET** button.

To reset the ES-305,

1 Make sure the **WAN/PWR LED** is on.
2 Press and hold the **RESET** button for about ten seconds. Release the **RESET** button.

If the ES-305 restarts automatically, wait for the ES-305 to finish restarting, and log in to the web configurator. By default, the ES-305 has no username or password; just click **OK** when you are asked for login information.

If the ES-305 does not restart automatically, disconnect and reconnect the ES-305's power. Then, follow the directions above again.

PART III
Appendices and Index

A

Product Specifications

The following tables summarize the ES-305's hardware and firmware features.

Table 10 Hardware Specifications

Dimensions (W x D x H)	125 x 85 x 25 mm
Power Specification	9V AC, 1A
Ethernet Ports	5 auto-negotiating, auto-crossover 10/100 Mbps full- or half-duplex fast Ethernet ports.
LEDs	LAN 1 ~ 3, LAN 4 / STATUS, WAN / PWR.
Operation Temperature	0º C ~ 50º C
Storage Temperature	-30º C ~ 70º C
Humidity	10% ~ 95% RH (non-condensing)

Table 11 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.0.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Username and Password	None
Device Management	Use the web configurator to easily configure the rich range of features on the ES-305.
VLAN	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.
Multicast VLAN Registration (MVR)	Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) using multicast traffic across a network. MVR allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.
Differentiated Services (DiffServ)	With DiffServ, the ES-305 marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow.
DSCP / IEEE 802.1p mapping	The ES-305 can add IEEE 802.1p values to traffic on the network based on their DSCP (DiffServ Code Point) value.

Table 11 Firmware Specifications

FEATURE	DESCRIPTION
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator or an FTP tool to put it on the ES-305. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ES-305's configuration. You can put it back on the ES-305 later if you decide to revert back to an earlier configuration.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ES-305 supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).

Table 12 Switching Specifications

Layer 2 Features	Bridging	1K MAC addresses
	Switching	Max. Frame size: 1522 bytes Forwarding frame: IEEE 802.3, IEEE 802.1q, Ethernet II
	QoS	802.1p, 2 egress priority queues Per port PVID setting SPQ queuing algorithm IGMP Snooping v1/v2 Fast Leave DiffServ (DSCP)
	VLAN	Tag-based (IEEE 802.1Q) VLAN Number of VLAN: 5 (static VLAN entries), full-range 4k PVID

The following list, which is not exhaustive, illustrates the standards supported in the ES-305.

Table 13 Standards Supported

STANDARD	DESCRIPTION
IEEE 802.1p	Traffic Types - Packet Priority
IEEE 802.1q	Tagged VLAN
IEEE 802.3	Packet Format
IEEE 802.3x	Flow Control
Safety	CSA 60950-1 EN 60950-1 IEC 60950-1
EMC	FCC Part 15 (Class A) CE EMC (Class A)

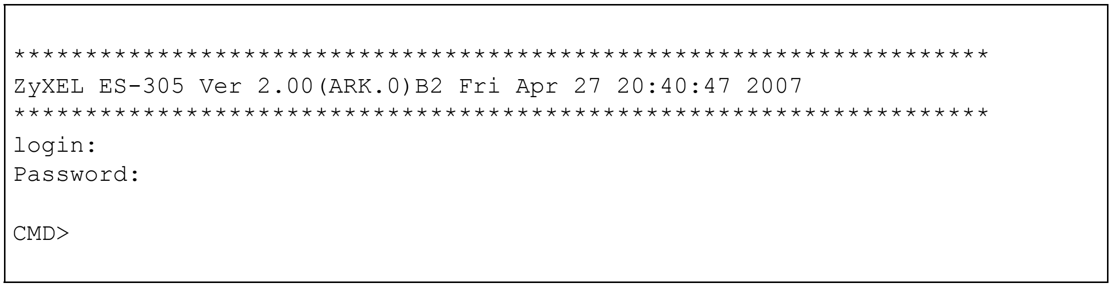
Connect to your ES-305 Using Telnet

The following procedure details how to telnet into your ES-305.

1 In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.0.1" (the default IP address) and click **OK**.

2 For your first login, just press **[Enter]** for the login (username) and password. If you already configured a username and password, enter them here. As you type the password, the screen displays an asterisk "*" for each character you type.

Figure 39 Login Screen



```
**********************************************************************
ZyXEL ES-305 Ver 2.00(ARK.0)B2 Fri Apr 27 20:40:47 2007
**********************************************************************
login:
Password:

CMD>
```

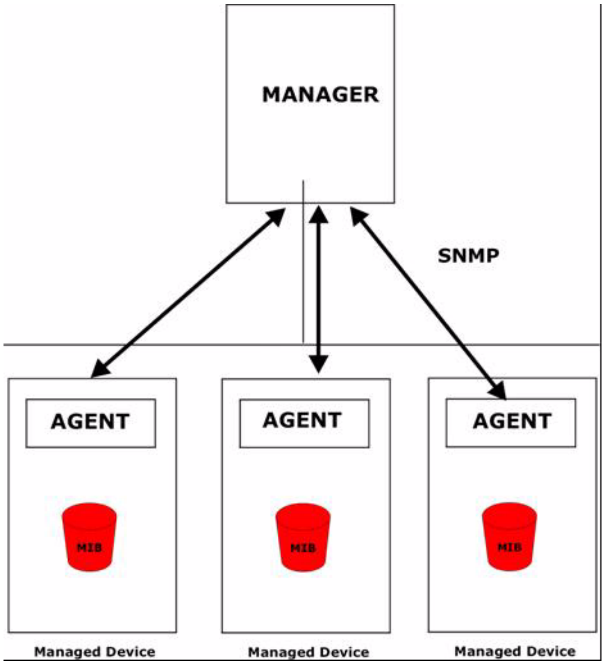
3 After entering the password, the `CMD>` command prompt indicates a successful login. Enter a question mark "`?`" to see a list of available commands.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your ES-305 will automatically log you out. You will then have to telnet into the ES-305 again. You can use the web configurator to change the inactivity time out period.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ES-305 supports SNMP agent functionality, which allows a manager station to manage and monitor the ES-305 through the network. The ES-305 supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 40 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ES-305). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the ES-305's physical ports.

Table 14 SNMP Interface Index to Physical and Virtual Port Mapping

INTERFACE	PORT
eth0	WAN
eth1	LAN 4
eth2	LAN 3
eth3	LAN 2
eth4	LAN 1

B

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

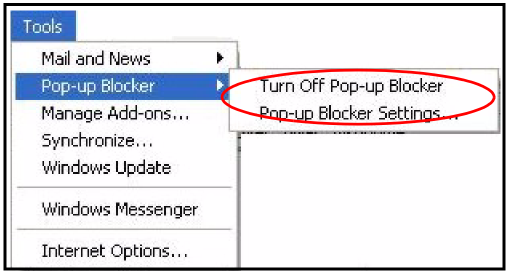
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 41 Pop-up Blocker

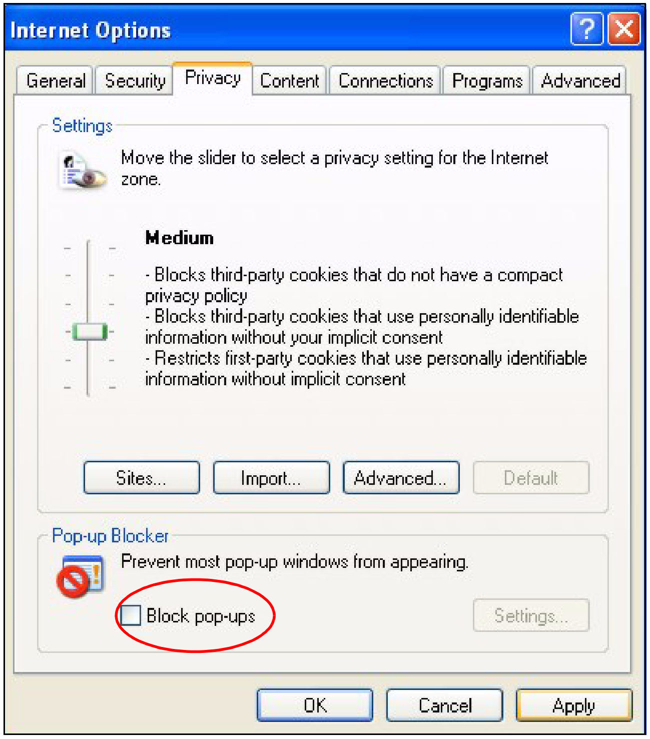


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 42 Internet Options: Privacy



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Sites... | Import... | Advanced... | Default

Pop-up Blocker

Prevent most pop-up windows from appearing.

□ Block pop-ups

Settings...

OK | Cancel | Apply

3 Click **Apply** to save this setting.

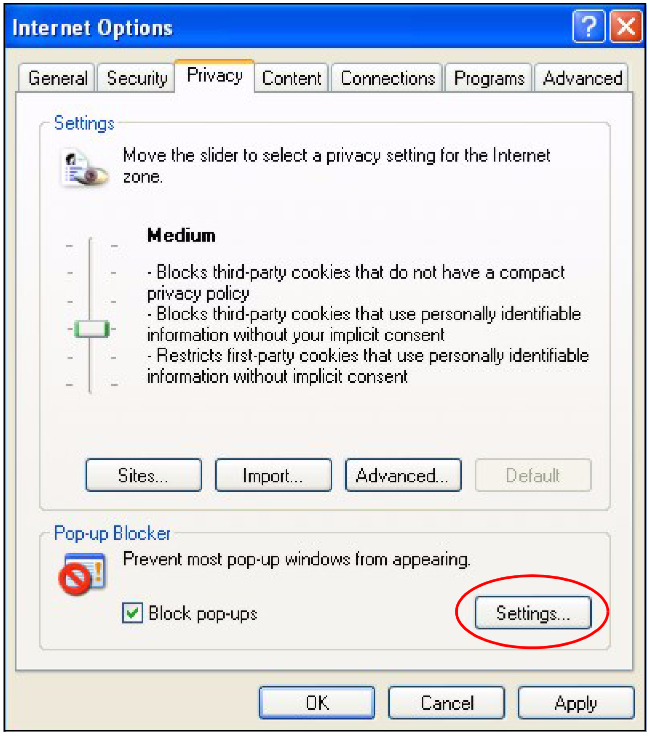
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 43 Internet Options: Privacy



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

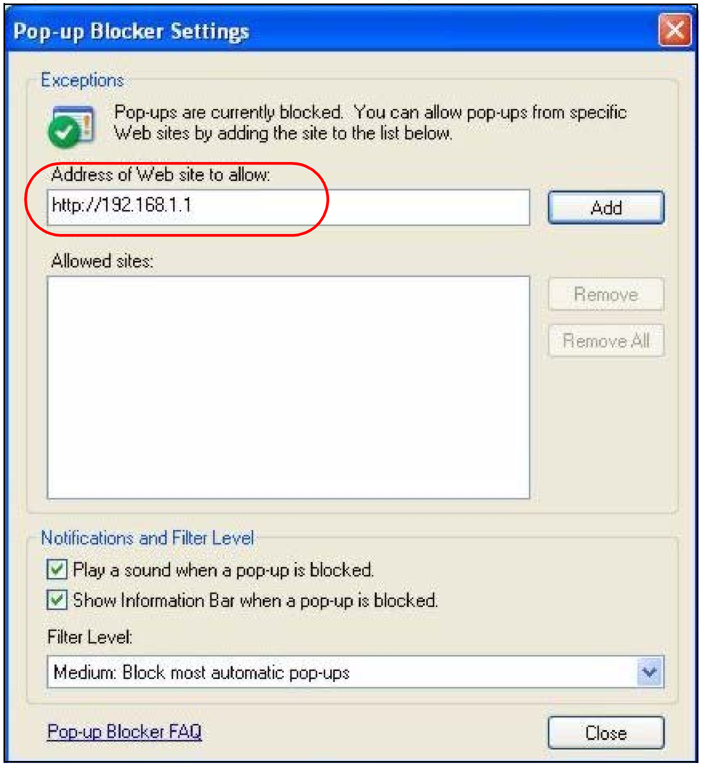
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 44 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow:

http://192.168.1.1

Allowed sites:

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level:

Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

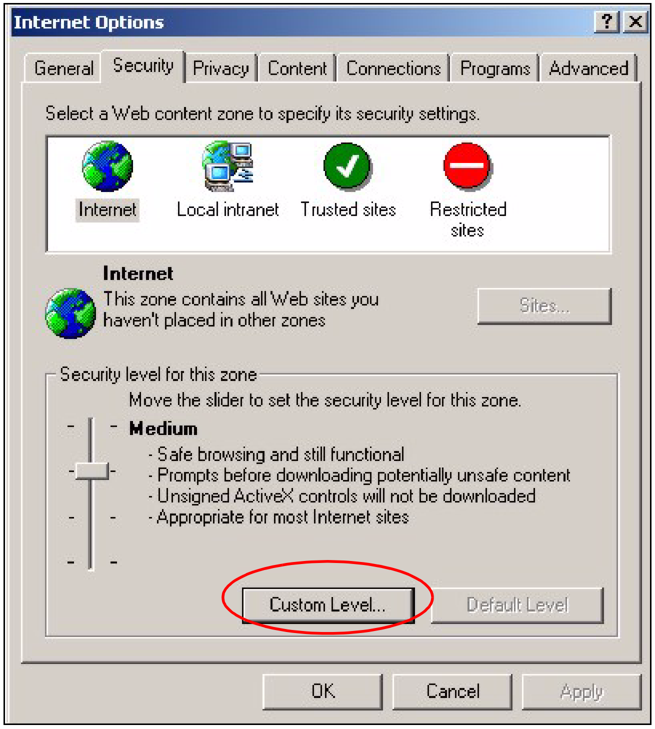
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 45 Internet Options: Security



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Move the slider to set the security level for this zone.

Medium

- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

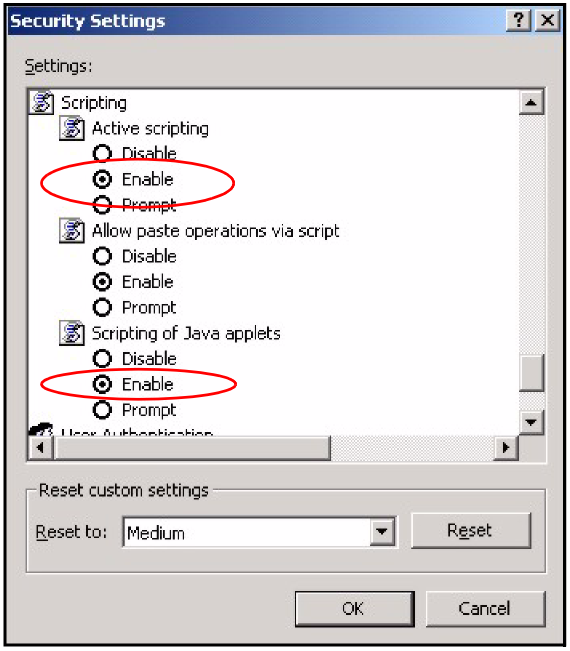
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 46 Security Settings - Java Scripting



Security Settings

Settings:

Scripting
Active scripting
○ Disable
● Enable
○ Prompt
Allow paste operations via script
○ Disable
● Enable
○ Prompt
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication

Reset custom settings

Reset to: Medium

Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

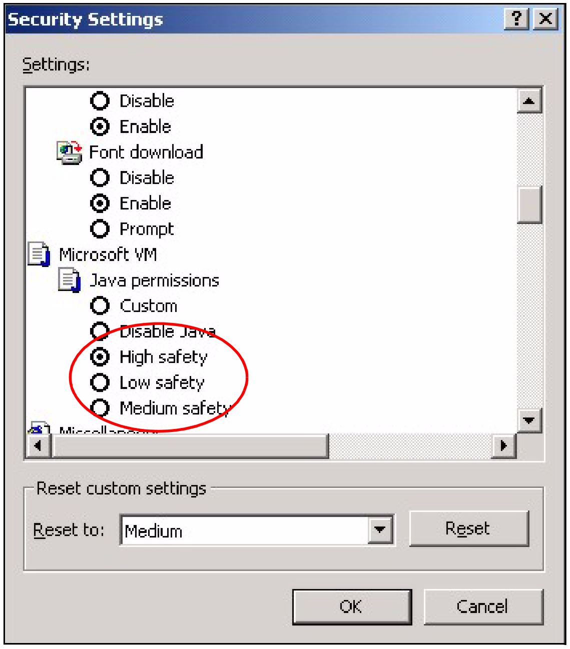
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 47 Security Settings - Java



Security Settings

Settings:

○ Disable
● Enable
Font download
○ Disable
● Enable
○ Prompt
Microsoft VM
Java permissions
○ Custom
○ Disable Java
● High safety
○ Low safety
○ Medium safety
Miscellaneous

Reset custom settings

Reset to: Medium

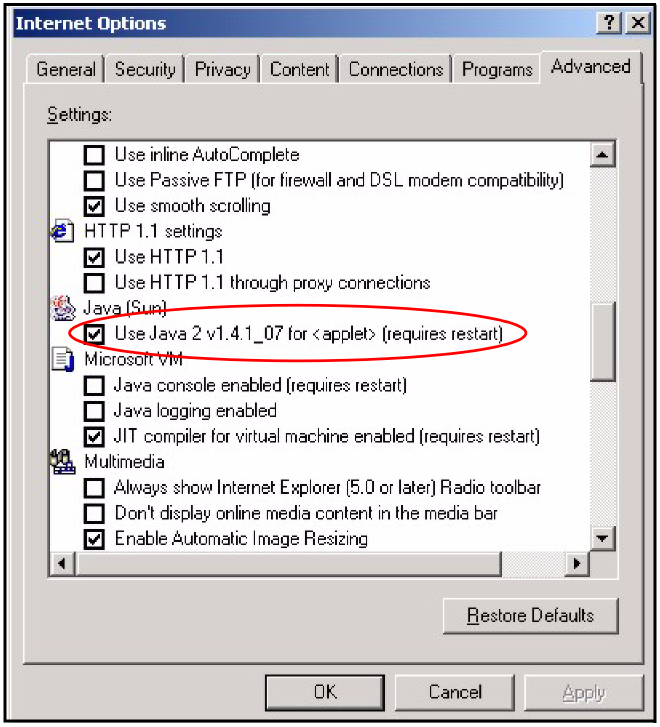
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 48 Java (Sun)



□ Use inline AutoComplete
□ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
□ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
□ Java console enabled (requires restart)
□ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
□ Always show Internet Explorer (5.0 or later) Radio toolbar
□ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

C

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

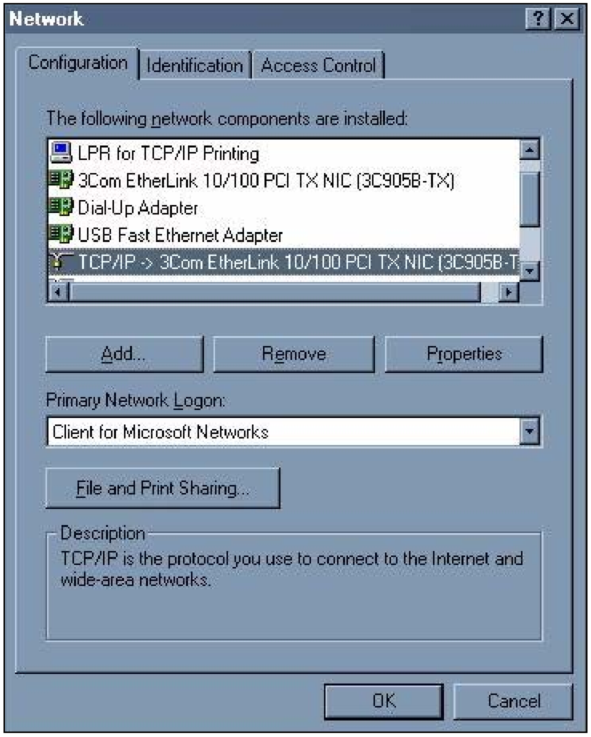
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ES-305's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 49 WIndows 95/98/Me: Network: Configuration



Network
Configuration
Identification
Access Control
The following network components are installed:
LPR for TCP/IP Printing
3Com EtherLink 10/100 PCI TX NIC (3C905B-TX)
Dial-Up Adapter
USB Fast Ethernet Adapter
TCP/IP -> 3Com EtherLink 10/100 PCI TX NIC (3C905B-T
Add...
Remove
Properties
Primary Network Logon:
Client for Microsoft Networks
File and Print Sharing...
Description
OK
Cancel

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.
2 Select **Adapter** and then click **Add**.
3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.
2 Select **Protocol** and then click **Add**.
3 Select **Microsoft** from the list of **manufacturers**.
4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.
2 Select **Client** and then click **Add**.
3 Select **Microsoft** from the list of manufacturers.
4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5 Restart your computer so the changes you made take effect.

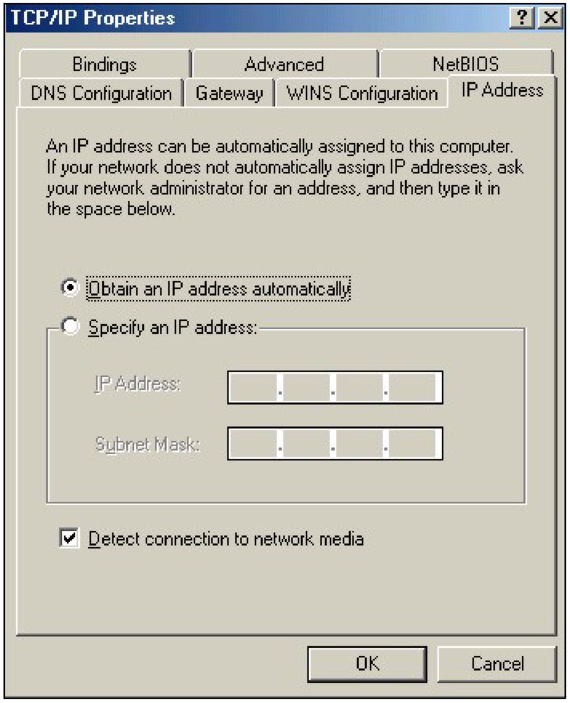
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 50 Windows 95/98/Me: TCP/IP Properties: IP Address



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

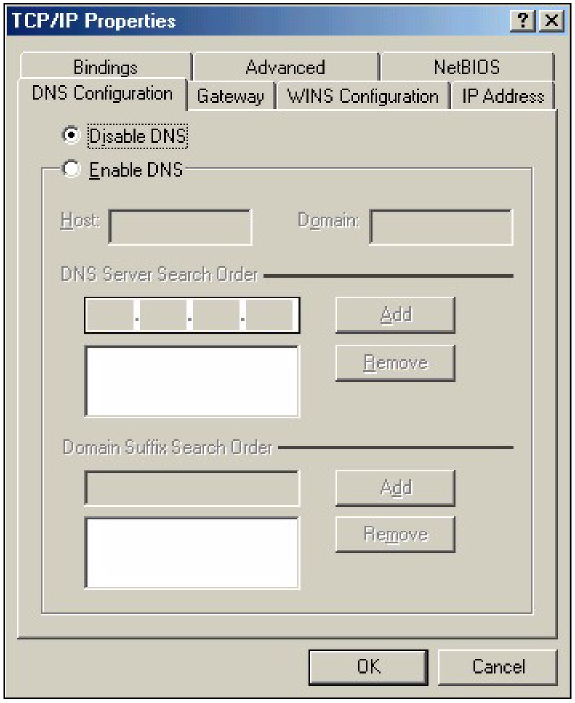
Subnet Mask: . . .

☑ Detect connection to network media

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 51 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



● Disable DNS

○ Enable DNS

4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your ES-305 and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

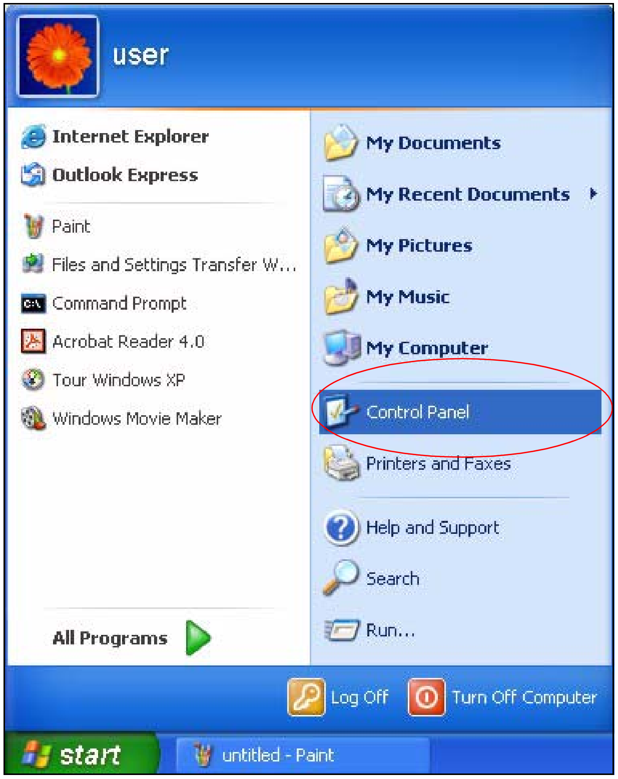
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

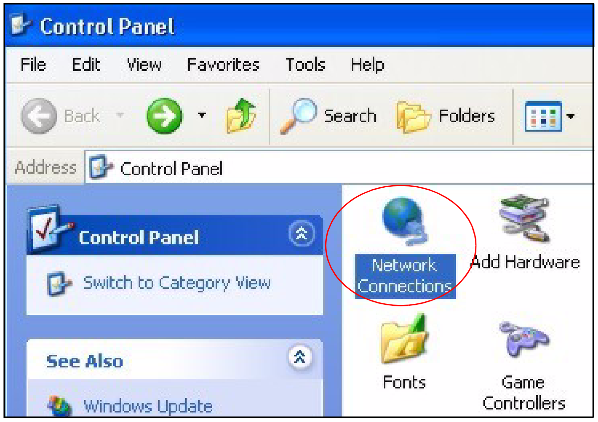
1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 52 Windows XP: Start Menu



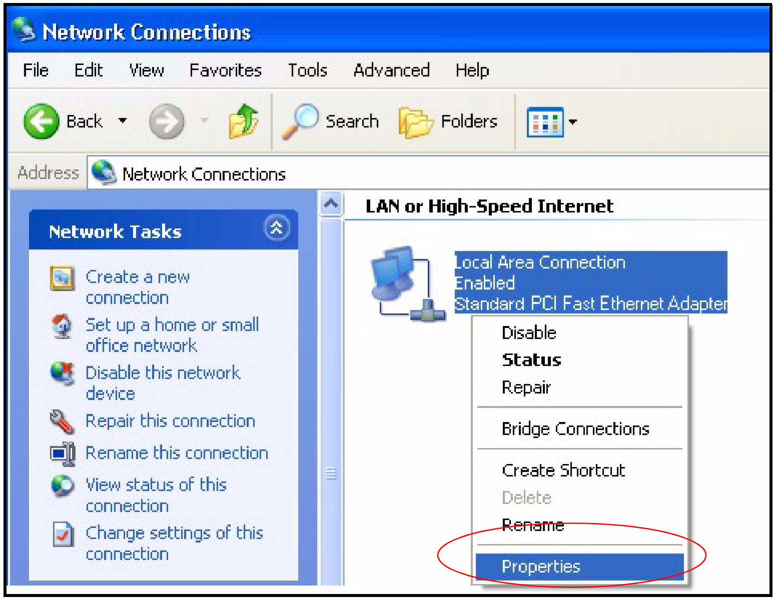
2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 53 Windows XP: Control Panel



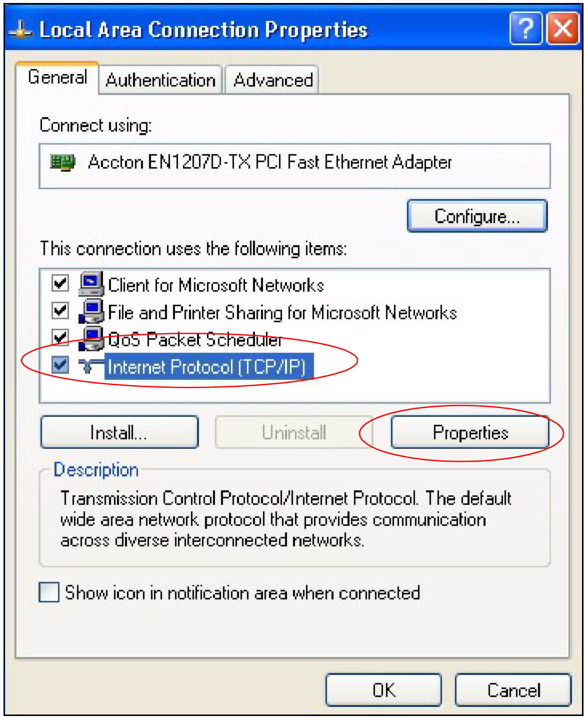
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 54 Windows XP: Control Panel: Network Connections: Properties


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 55 Windows XP: Local Area Connection Properties


Local Area Connection Properties
General Authentication Advanced
Connect using:
Configure...
This connection uses the following items:
Install... Uninstall Properties
Description
OK Cancel

Accton EN1207D-TX PCI Fast Ethernet Adapter

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

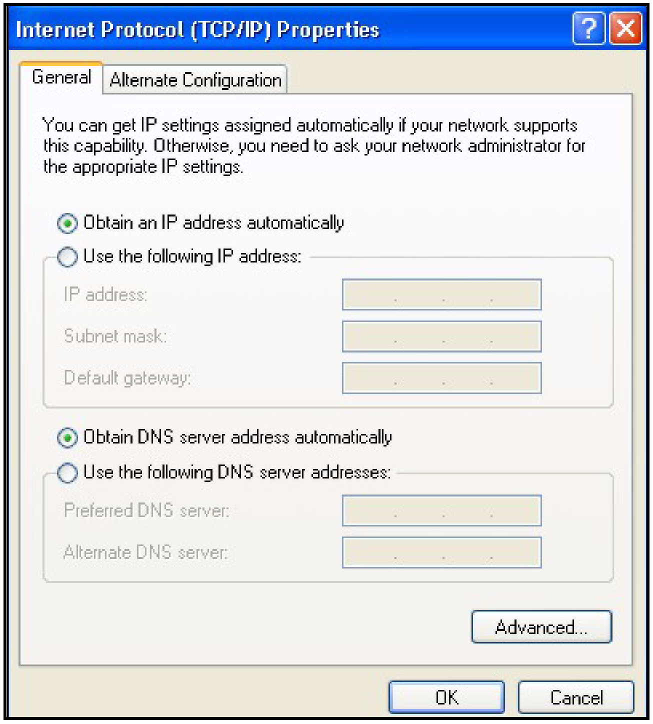
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 56 Windows XP: Internet Protocol (TCP/IP) Properties



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

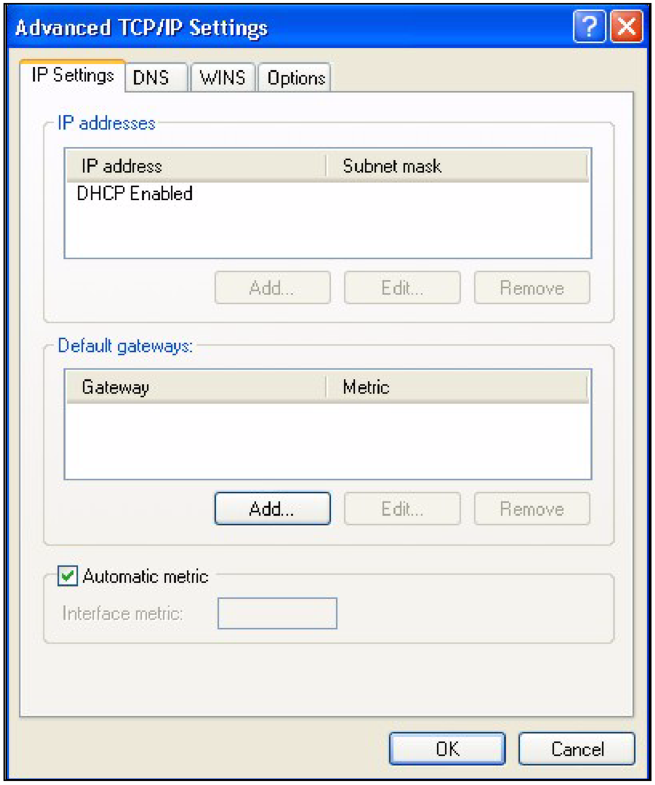
Alternate DNS server: . . .

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 57 Windows XP: Advanced TCP/IP Properties



DHCP Enabled

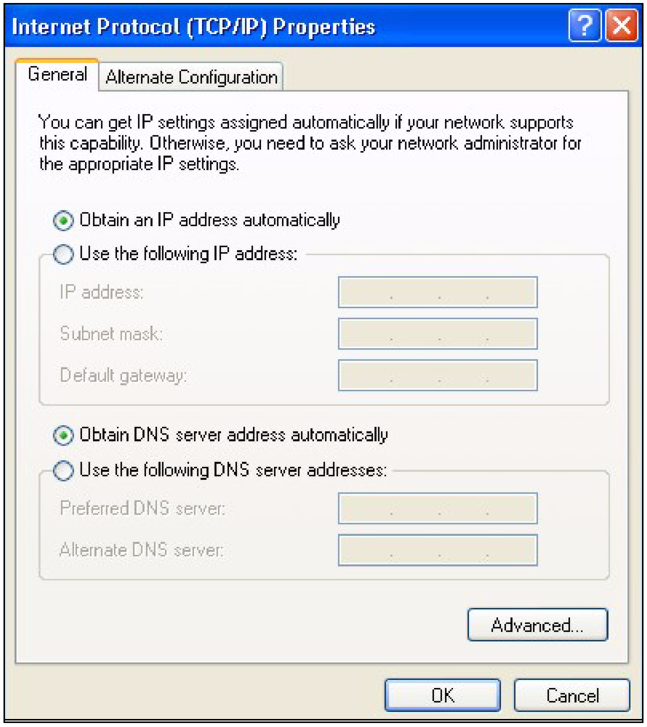
☑ Automatic metric

7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 58 Windows XP: Internet Protocol (TCP/IP) Properties



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ES-305 and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

D

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

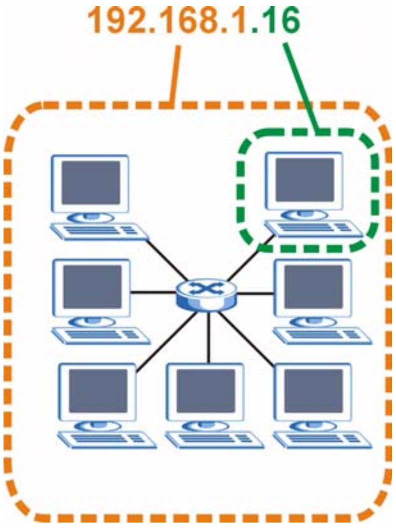
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 59 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 15 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 16 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 17 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 18 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 18 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

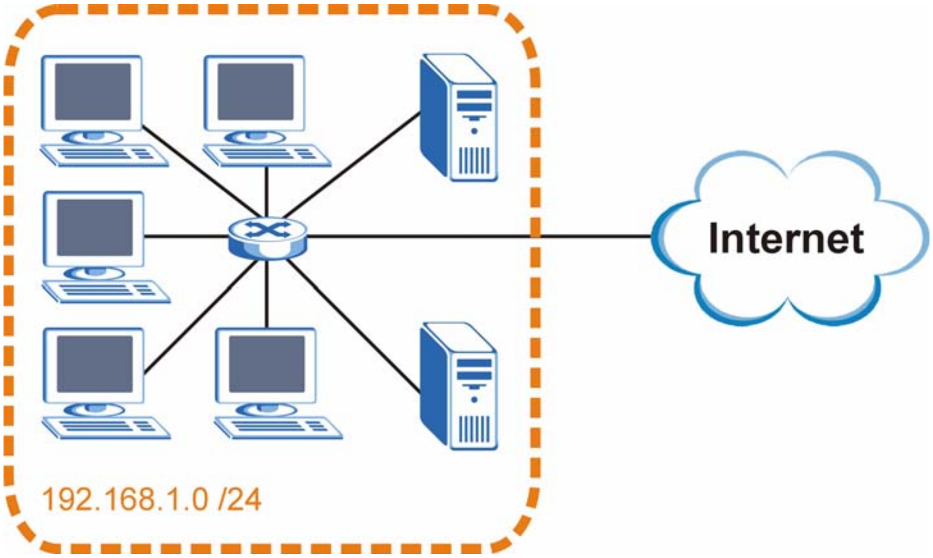
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 – 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 60 Subnetting Example: Before Subnetting

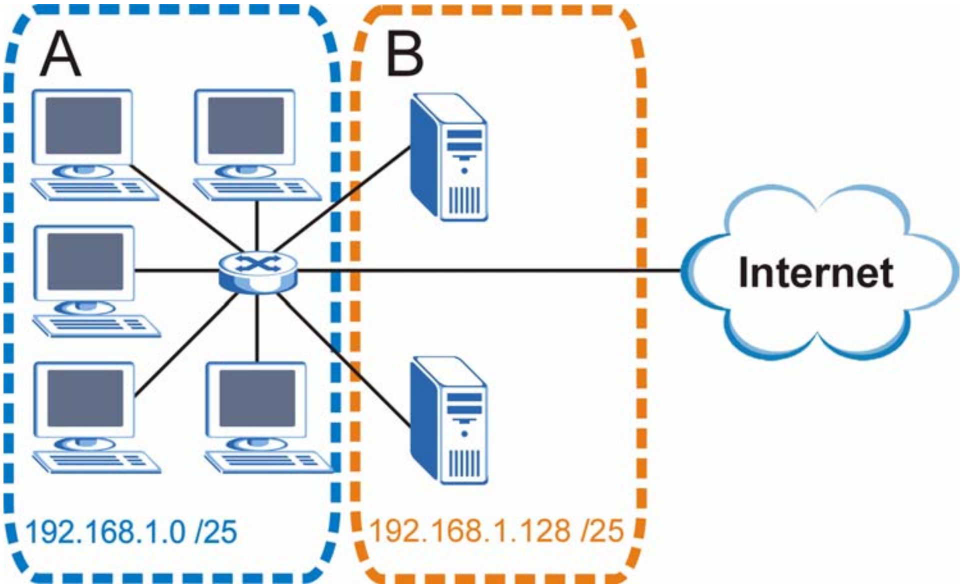


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 61 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 19 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 20 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 21 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 22 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 23 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 23 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 24 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 25 16-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 25 16-bit Network Number Subnet Planning (continued)

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ES-305.

Once you have decided on the network number, pick an IP address for your ES-305 that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ES-305 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ES-305 unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

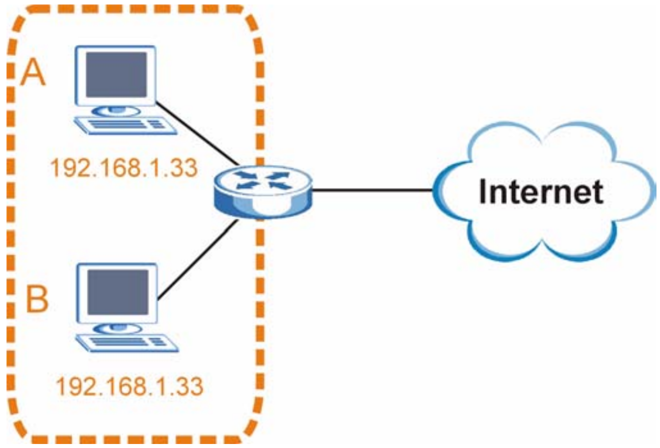
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

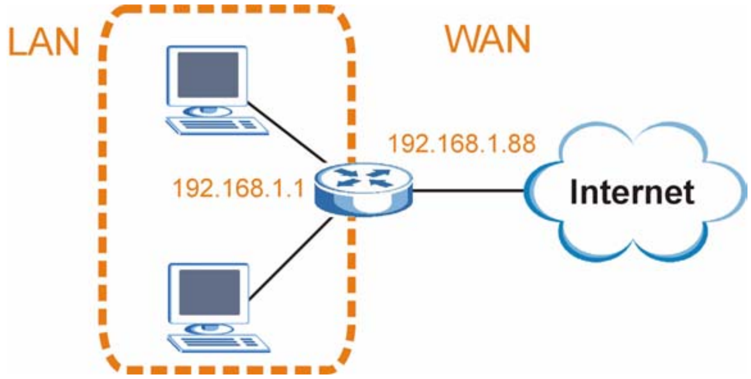
Figure 62 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

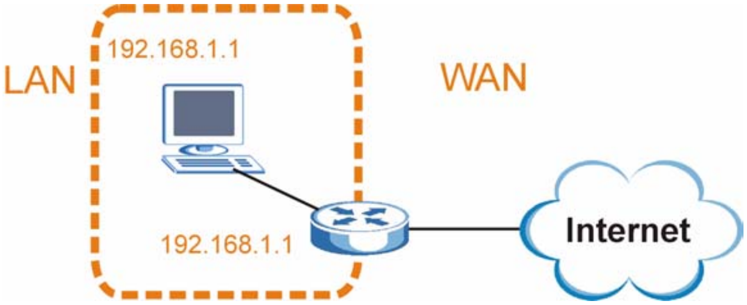
Figure 63 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 64 Conflicting Computer and Router IP Addresses Example



Command Interpreter

The following describes how to use the command interpreter. See the section on Telnet in Appendix A on page 69 for how to log into the command interpreter.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets [].
- The | symbol means "or".

  For example,

  ```
  sys filter netbios config <type> <on|off>
  ```

  means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

- A list of valid commands can be found by typing `help` or `?` at the command prompt.
- Always type the full command.
- The ES-305's command interface structure is hierarchical; type `up` to return to the previous command level.
- Type `quit` to close the session when finished.

Command Examples

This section provides some examples of commands you can use on the ES-305. This list is intended as a general reference of examples. The commands available in your ES-305 may differ from the examples given here.

Root Directory

When you first log in to the command interface, you are in the root directory. The CMD> prompt displays. From here you can access all of the ES-305's command directories. The command directories are as follows.

- cfg: these commands manage configuration settings.
- net: these commands manage Internet settings.
- os: these commands manage operating system settings.

Commands Summary

The following table illustrates the commands available in the ES-305's command interface.

Table 26 Commands Summary

`cfg`	`get <var>`		Displays the specified profile variable (use `cfg prof show` to see all profile variables).
			Variable names are case-sensitive.
			Example (displays current SNMP contact person data):
			`CFG> get SNMP_SYSCONTACT`
			`SNMP_SYSCONTACT=admin@1234.com`

	`set <var>`		Sets the specified profile variable to runtime memory (use `cfg prof show` to see all profile variables). Variable names are case-sensitive. Example (sets system login password to “4321”): `CFG> set SYS_ADMPASS 4321` Use the `cfg prof commit` command to save changes to non-volatile memory.

	`del <var>`		Deletes the specified variable.
			Example (deletes the SNMP system location variable):
			`CFG> del SNMP_SYSLOC`

	`prof`		These commands let you see and save changes to the ES-305’s profile (its configuration settings).
		`init`	Return profile to initial factory default settings. All configuration changes are lost.
		`save`	Save all current profile settings to non-volatile memory.
		`commit`	Save changes made via the `cfg set` command to non-volatile memory.
		`show`	Display the current profile.
	`restore <server-ip> <filename>`		Restores a specified profile from the specified IP address. Example (restores profile “profile.bin” from the server at 10.10.10.10): `CFG> restore 10.10.10.10 profile.bin`
	`backup`		Saves the current profile to the specified file on the specified server via TFTP. Example (saves the current profile as “profile2.bin” to the server at 10.10.10.10): `CFG> backup 10.10.10.10 profile2.bin`

Table 26 Commands Summary

`net`	`show`	`stat`	Displays network monitor information and statistics for transmitted and received packets.
		`kmem`	Displays kernel memory statistics.
		`route`	Displays routing tables and interface statistics.
		`eth0`	Displays information about the **WAN** port.
		`eth1`	Displays information about the **LAN4** port.
		`eth2`	Displays information about the **LAN3** port.
		`eth3`	Displays information about the **LAN2** port.
		`eth4`	Displays information about the **LAN1** port.
	`br`	`start`	Turn bridging on.
		`stop`	Turn bridging off.
		`restart`	Restart bridging.
		`show`	Display bridging status.
	`vlanconfig`		Use this command to see the Virtual LAN (Port VID and IEEE 802.1p priority) status of the ES-305's ports.

		`<port_name> [<pvid>]`	Use this command to see the VLAN status of the specified port. Add the `<pvid>` in order to assign the the specified Port VLAN ID to the port.
			Example (assigns PVID 12 to port 2x):
			`NET> vlanconfig 2x 12`

		`<port_name> priority <priority>`	Use this command to see the IEEE 802.1p priority of the specified port. Add the `priority <priority>` to assign the specified IEEE 802.1p priority to the port.
			Example (assigns IEEE 802.1p priority 3 to port 3x):
			`NET> vlanconfig 3x priority 3`

	`ping <dst-ip> [<timeout>] {<loop>]`		Use this command to ping other devices on the network.
			Example:
			`NET> ping 10.10.10.10 3 5`
			`seq:0 rtt=0`
			`seq:1 rtt=0`
			`seq:2 rtt=1`
			`seq:3 rtt=0`
			`seq:4 rtt=0`

	`arp`	`show`	Displays current Address Resolution Protocol table entries.
		`flush`	Clears all Address Resolution Protocol table entries.
	`http`	`logout`	Use this command to log off an http user logged in to the ES-305's web configurator.

Table 26 Commands Summary

os	thread		Use this command to see details and statistics of all threads currently running on the ES-305.
	mem		Use this command to see the total and available memory on the ES-305
	rst		Use this command to reboot the ES-305. Note that this command does not reset the device to its default configuration.

F

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

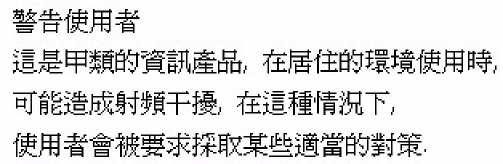
FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:



警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策．

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Viewing Certifications

1 Go to http://www.zyxel.com.
2 Select your product on the ZyXEL home page to go to that product's page.
3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

G

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web Site: www.zyxel.com, www.europe.zyxel.com
- FTP Site: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web Site: www.zyxel.co.cr
- FTP Site: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web Site: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web Site: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780 8448
- Web Site: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web Site: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web Site: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web Site: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz

- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web Site: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web Site: www.us.zyxel.com
- FTP Site: ftp.us.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web Site: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48 (22) 333 8250
- Fax: +48 (22) 333 8251
- Web Site: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web Site: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow, 117279, Russia

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345

- Web Site: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web Site: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web Site: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev, 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344 303044, 08707 555779 (UK only)
- Fax: +44-1344 303034
- Web Site: www.zyxel.co.uk
- FTP Site: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK, Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

"+" is the (prefix) number you dial to make an international telephone call.

Index